이학박사 학위논문

On some conjectures on the arithmetic of elliptic curves

(타원 곡선의 수론에 관한 몇 가지 가설들)

2016년 2월

서울대학교 대학원

수리과학부

김태경

On some conjectures on the arithmetic of elliptic curves

(타원 곡선의 수론에 관한 몇 가지 가설들)

지도교수 변동호

이 논문을 이학박사 학위논문으로 제출함

2015년 12월

서울대학교 대학원

수리과학부

김태경

김태경의 이학박사 학위논문을 인준함

2015년 12월

위 원 장 _____ (인)

부 위 원 장 _____ (인)

위 원 _____ (인)

위 원 _____ (인)

위 원 _____ (인)

On some conjectures on the arithmetic of elliptic curves

A dissertation
submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
to the faculty of the Graduate School of
Seoul National University

by

Taekyung Kim

Dissertation Director : Professor Dongho Byeon

Department of Mathematical Science
Seoul National University

February 2016

Abstract

On some conjectures on the arithmetic of elliptic curves

Taekyung Kim

Department of Mathematical Sciences
The Graduate School
Seoul National University

The goal of the present thesis is twofold; we show the two conjectures concerning the arithmetic of elliptic curves: the Stein–Watkins conjecture (for 5-isogenies) and the Gross–Zagier conjecture.

Essentially, Stein–Watkins conjecture tells us about the relations of optimal curves in given rational isogeny class of elliptic curves. In this thesis we show the two optimal curves differ by a 5-isogeny if and only if the isogeny class is '11a'.

The Gross–Zagier conjecture provides a theoretical evidence to the strong form of Birch and Swinnerton-Dyer conjecture. We show when elliptic curves have particular types of rational torsion subgroups, the order of the torsion subgroup divides certain arithmetic invariants attached to the curve.

Key words: elliptic curves, Birch and Swinnerton-Dyer conjecture, Gross–Zagier theorem, isogeny of elliptic curves
Student Number: 2009–20265

Contents

Chapter 1

Introduction

> "Charm was a scheme for making strangers like and trust a person immediately, no matter what the charmer had in mind."
>
> Kurt Vonnegut,
> *Breakfast of Champions*

Since the beginning of the history of mathematics, *Diophantine equations*, i.e. systems of polynomial equations with integer or rational coefficients in one or several unknown variables, is at the centre of mathematicians' interest. Diophantine problems ask to seek solutions to such Diophantine equations, in any available methods known.

One natural way to study Diophantine equations makes use of algebraic geometry. Because algebraic geometry is the algebraic study of geometric properties of loci defined by polynomial equations and so provides plenty of methodologies to Diophantine problems. This interesting mixture of geometry and arithmetic have grown exponentially, especially after Grothendieck's revolution, and at last it coined the words "arithmetic geometry" and "Diophantine geometry" having similar meanings: utilizing algebraic geometry

to study the arithmetic of Diophantine equations. Let us give an example showing how geometry prevails in the realm of Diophantine equations.

Since there are a vast amount of Diophantine equations to study, mathematicians have been seeking some taxonomy of the equations. For Diophantine equations defining projective curves, we indeed have one; it is an invariant called *genus of the curve*, which is a non-negative integer g. When $g = 1$, the curve is essentially a projective line $\mathbf{P}^1$, thus the rational points can be sought easily. Meanwhile when $g \geq 2$, Faltings' amazing theorem says that there are finitely many rational points. For the remaining bounded case, when $g = 1$, the curve is one of the most beautiful object in mathematics, the elliptic curves or its twists.

The arithmetic of elliptic curves is the subject of this thesis. We will see lots of interesting properties of elliptic curves on algebro-geometric, algebraic, and analytic sides of view. After developing enough terminologies, notions and concepts in chapter I, we directly dive into two interesting conjectures in the arithmetic of elliptic curves.

The first conjecture we deal with is called Stein–Watkins conjecture, which tells us about the relations between optimal curves. There are two kinds of optimal curves in any isogeny class of elliptic curves. The first one, the $X_0(N)$-optimal curve is classical, and it is also called the *strong Weil curve*. The existence of this curve is due to modularity theorem, whose proof was located at the peak of human study on number theory in the 20th century. The second kind is the $X_1(N)$-optimal curve, and conjecturally this has some intrinsic characterisation. We hope the discovery of the relations between these two optimal curves will provide lots of theoretical and computational applications. We prove the 5-isogeny case of the Stein–Watkins conjecture in this thesis, remaining others to future research.

The second is Gross–Zagier conjecture, which gives a theoretical evidence to Birch and Swinnerton-Dyer conjecture, which we dare to call the most important conjecture in the arithmetic of elliptic curves. Besides such effects

of the result, the process of proof also gives lots of inspirations to study further. There are plenty of topics and questions related to the Gross–Zagier conjecture remained unanswered; we hope to go further in this direction in the future.

Notations and conventions

Let K be a field. We denote the algebraic (resp. separable) closure of K by $\overline{K}$ (resp. K^{sep}). So in particular for perfect fields, $\overline{K} = K^{\mathrm{sep}}$. We let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group over K. As usual, when M is a G_K-module, the Galois cohomology groups $H^q(G_K, M)$ are often abbreviated to $H^q(K, M)$.

By a *variety* X we mean an integral separated scheme of finite type over a field K. Usually when thinking of varieties, it is identified with the set of closed points of the variety, i.e., the elements of the set $X(\overline{K})$ by Nullstellensatz (cf. [Mum], §II.4). A *curve* is an algebraic variety of dimension 1.

All theorems, propositions in this thesis are numbered as `cc.nn` where `cc` is the number of the chapter at which the item is located, and `nn` is the number of the item.

Chapter 2

Elliptic curves

> "He who has not first laid his foundations may be able with great ability to lay them afterwards, but they will be laid with trouble to the architect and danger to the building."
>
> Niccolò Machiavelli,
> *The Prince*

In this chapter we introduce basic notions concerning the arithmetic of elliptic curves. Of course, none of the materials in this chapter is original. These are well treated in numerous literature, including texts of Silverman ([Sil97], [Sil94] and [Sil09]), Milne ([Mil06]), or Knapp ([Kna]). Proofs of the theorems will be only given in some simple or 'too-important-to-be-ignored' cases; otherwise we give precise references at which the proofs can be found.

2.1 Fundamentals on elliptic curves

Definition. An *elliptic curve* E over a perfect field K (e.g. number fields, local fields arising from completions of number fields, or finite fields) is a smooth projective curve of genus 1 defined over K, with a specified rational point $O \in E(K)$.

Finding rational points of E (elements in $E(K) = E^{G_K}$) is a Diophantine problem; we can embed E as a smooth cubic curve in $\mathbf{P}^2$ given by the following homogeneous equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{2.1}$$

where $a_1, \cdots, a_6 \in K$, and $\Delta \neq 0$ (see below for the precise definition of Δ).

Equation (2.1) is called the *Weierstrass equation*. For convenience, we dehomogenise the equation (2.1) by setting $x = X/Z$ and $y = Y/Z$, and call the resulting equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.2}$$

the *(affine) Weierstrass equation*.

When a Weierstrass equation is given, we define the following quantities.

- $b_2 = a_1^2 + 4a_2$,
- $b_4 = 2a_4 + a_1a_3$,
- $b_6 = a_3^2 + 4a_6$,
- $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$,
- $c_4 = b_2^2 - 24b_4$,
- $c_6 = -b_2^2 + 36b_2b_4 - 216b_6$,
- $\Delta = -b_2^2b_8 - 8b_4^3 27b_6^2 + 9b_2b_4b_6$ (the *discriminant* of the equation (2.1)),

- $j = c_4^3/\Delta$ (called the *j-invariant*),
- $\omega = dx/(2y + a_1x + a_3) = dy/\left(3x^2 + 2a_2x + a_4 - a_1y\right)$ (the *invariant differential* associated to the equation (2.1)).

The equation (2.1) has a trivial K-point $[0, 1, 0]$, which is the only point in the intersection of the locus the equation (2.1) defines and the locus of the equation $Z = 0$. Classically, this point is called the *point at infinity*, and corresponds to the point $O \in E(K)$ in the definition of elliptic curves. In particular, when we are given an affine Weierstrass equation (2.2), the point $[0, 1, 0]$ can be written as $\infty \in E(K)$.

Two distinct Weierstrass equations can define the same elliptic curve. Given an affine Weierstrass equation (2.2), the only change of variables fixing the point at infinity $[0, 1, 0]$ and preserving the Weierstrass form is

$$x = u^2x' + r, \qquad y = u^3y' + u^2sx' + t,$$

where $u, r, s, t \in \overline{K}$ and $u \neq 0$. We will frequently make use of such changes in order to work with more convenient form. Throughout, we refer this change of variables as "the change of variables via $[u, r, s, t]$". After such a change, Weierstrass coefficients and important constants are changed as summarised in Table 2.1.

The most important feature on the arithmetic of elliptic curves is that the points of an elliptic curve form an abelian group. This group structure comes from the divisor group of the elliptic curve as an algebraic curve.

Let C/K be an algebraic curve defined over K. We denote by $\mathrm{Div}(C)$ (resp. $\mathrm{Div}^0(C)$) the *(Weil) divisor group* of C, i.e. the free abelian group generated by points of C (resp. the group of divisors of degree 0). Also, $\mathrm{Pic}(C)$ (resp. $\mathrm{Pic}^0(C)$) is the quotient group of $\mathrm{Div}(C)$ (resp. $\mathrm{Div}^0(C)$) modulo linear equivalence relation. The group structure of an elliptic curve E is defined in terms of these groups.

a'_1	$= u^{-1}(a_1 + 2s)$
a'_2	$= u^{-2}\left(a_2 - sa_1 + 3r - s^2\right)$
a'_3	$= u^{-3}(a_3 + ra_1 + 2t)$
a'_4	$= u^{-4}\left(a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st\right)$
a'_6	$= u^{-6}\left(a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1\right)$
b'_2	$= u^{-2}(b_2 + 12r)$
b'_4	$= u^{-4}\left(b_4 + rb_2 + 6r^2\right)$
b'_6	$= u^{-6}\left(b_6 + 2rb_4 + r^2b_2 + 4r^3\right)$
b'_8	$= u^{-8}\left(b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4\right)$
c'_4	$= u^{-4}c_4$
c'_6	$= u^{-6}c_6$
Δ'	$= u^{-12}\Delta$
j'	$= j$
ω'	$= u\omega$

Table 2.1: Change of variables formula, copied from the Table 3.1 in [Sil09].

Theorem 2.1 (Proposition III.3.4 in [Sil09])**.** *Let E be an elliptic curve over K. Then there is a bijection*

$$\kappa : E \xrightarrow{\sim} \mathrm{Pic}^0(E), \qquad P \longmapsto (\textit{divisor class of } (P) - (O))$$

preserving the action of G_K. Therefore, we can import the group structure from $\mathrm{Pic}^0(E)$ *to E.*

This group structure on E coincides with the classical one from chord-tangent group law (cf. Theorem III.3.6 in [Sil09]). This group structure is defined over K, i.e., an elliptic curve together with the group structure is an algebraic group over K.

2.2 Isogenies, endomorphism rings and twists

An *isogeny* is a non-constant morphism (as algebraic curves) $\phi : E \longrightarrow E'$ between two elliptic curves E and E' which is also a group homomorphism. In fact, isogenies can be defined by much weaker condition.

Theorem 2.2. *Let $\phi : E \dashrightarrow E'$ be a non-constant rational map between elliptic curves such that $\phi(O) = O$. Then ϕ is an isogeny.*

Proof. A rational map between smooth projective curves is a morphism, see Proposition III.2.1 in [Sil09]. See Theorem III.4.8 *op. cit.* for the group homomorphism property. □

The degree of an isogeny ϕ is the degree as a finite map of curves, or equivalently, the degree is the degree of extension of function fields of two curves. (Two function fields are related via the pullback map defined by ϕ.) Conventionally, the constant map sending all the points of E to O is set to have degree 0.

Example 2.3. Let E be an elliptic curve defined over K. For each integer m, we can define the *multiplication-by-m map* $[m] : E \longrightarrow E$ by sending $P \in E$ to

$$[m](P) = \begin{cases} P + \cdots + P \ (m \text{ summands}) & \text{if } m > 0, \\ O & \text{if } m = 0, \\ (-P) + \cdots + (-P) \ (-m \text{ summands}) & \text{if } m < 0. \end{cases}$$

When $m \neq 0$, the multiplication-by-m maps are isogenies of degree m^2. We write

$$E[m] = \ker[m] = \{P \in E : [m](P) = O\}.$$

This is a finite subgroup of E. Note that the maps $[m]$ for each $m \in \mathbf{Z}$ are also defined over K. In particular, this means the subgroup $E[m]$ is invariant under the action of G_K, i.e., $E[m]$ is a finite Galois module over K.

If there is an isogeny $\phi : E \longrightarrow E'$, then we say E and E' are *isogenous*. This is an equivalence relation: when ϕ is given, we can find the *dual isogeny* $\phi' : E' \longrightarrow E$ satisfying $\phi' \circ \phi = [m]$ and $\phi \circ \phi' = [m]$, where m is the degree of ϕ. Dual isogenies have the following properties:

$$\phi'' = \phi, \quad (\phi + \psi)' = \phi' + \psi', \quad (\phi \circ \psi)' = \psi' \circ \phi', \quad [m]' = [m].$$

A *(rational) isogeny class* C is an equivalence class of isogenous curves over $\mathbf{Q}$.

As usual, two elliptic curves E/K and E'/K are said to be *isomorphic* over K if there are isogenies $\phi : E \longrightarrow E'$ and $\psi : E' \longrightarrow E$ defined over K such that $\phi \circ \psi$ and $\psi \circ \phi$ are identity maps. As every isogeny has its dual, two curves are isomorphic if and only if they are isogenous via an isogeny of degree 1.

Here, the reference to the field K is crucial: two curves E and E' may not isomorphic over a field K but become isomorphic over some extension field of K. In this case, we say E' is a *twist* of E (or vice versa). This can be studied via Galois cohomology. Suppose that an (geometric or algebraic) object X is given and is defined over a field K, and let L be a finite Galois extension of K. Then the K-isomorphism classes of objects defined over K which are L-isomorphic to X are in one-to-one correspondance to the elements of the cohomology group $H^1(\mathrm{Gal}(L/K), \mathrm{Aut}(X/L))$, where $\mathrm{Aut}(X/L)$ is the group of L-automorphisms of X/L. This is a typical situation, and for more informations we refer to texts on Galois cohomology, e.g. chapter X in [Ser79].

In order to classify twists of given elliptic curve E, we have to find the automorphism group $\mathrm{Aut}(E)$. First, we consider the endomorphism rings.

Theorem 2.4. *Let E be an elliptic curve over a field K.*

(i) The endomorphism ring of E is one of the following sort of rings:

$$\mathrm{End}(E) = \begin{cases} \mathbf{Z}, \\ \textit{an order in an imaginary quadratic field}, \\ \textit{a maximal order in a quaternion algebra over } \mathbf{Q}. \end{cases}$$

The third possibility only occurs when $\mathrm{char}(K) > 0$.

(ii) Assume $\mathrm{char}(K) = 0$. *Then the automorphism group of E is one of the following sort of groups:*

$$\mathrm{Aut}(E) = \begin{cases} \mu_2 & \textit{if } j \neq 0, 1728, \\ \mu_4 & \textit{if } j = 1728, \\ \mu_6 & \textit{if } j = 0. \end{cases}$$

Proof. Theorem III.9.3 and Corollary III.10.2 in [Sil09]. □

Thus, in particular, when E is defined over $\mathbf{Q}$ and $j \neq 0, 1728$, then by Kummer theory we have

$$H^1(\mathbf{Q}, \mathrm{Aut}(E)) = H^1(\mathbf{Q}, \mu_2) = \mathbf{Q}^\times / \mathbf{Q}^{\times 2},$$

and thus each representative $d \in \mathbf{Q}^\times$ modulo $\mathbf{Q}^{\times 2}$ define a twist of E, called the *quadratic twist* E_d of E. When E is given by the Weierstrass equation[1]

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6,$$

the curve E_d is given by

$$dy^2 = x^3 + a_2 x^2 + a_4 x + a_6,$$

[1]When $\mathrm{char}(K) \neq 2$, every Weierstrass equation defining E can be transformed into this form, cf. Remark below Theorem 2.7.

or equivalently,

$$y^2 = x^3 + da_2x^2 + d^2a_4x + d^3a_6.$$

When E has endomorphism ring strictly larger than $\mathbf{Z}$, we say E has *complex multiplication* (*CM* for short). Elliptic curves with CM has many applications on classical and modern branches in number theory. For detailed expositions on CM elliptic curves, we refer to chapter II of [Sil94] and Serre's short treatise [Ser67].

2.3 Torsion points

The torsion subgroup of E is the set of all points of finite order,

$$E_{\text{tors}} = \bigcup_{m \geq 1} E[m] = \{P \in E : [m]P = O \text{ for some } m \geq 1\}.$$

At least as an abstract group, the structure of the torsion group is well-known.

Theorem 2.5. *Let E/K be an elliptic curve.*

(i) If $\text{char}(K) = p \geq 0$ *with* $p \neq m$, *then as abstract groups,*

$$E[m] \cong \mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z}.$$

(ii) If $\text{char}(K) = p \neq 0$, *then for each* $r \geq 1$,

$$E[p^r] = \begin{cases} \mathbf{Z}/p^r\mathbf{Z}, \text{ or} \\ 0. \end{cases}$$

Proof. Corollary III.6.4 in [Sil09]. □

When $\text{char}(K) = p \neq 0$, the triviality of the group $E[p^r]$ is independent of r. We say *E is ordinary at p* (or *p is an ordinary prime of E*) if $E[p^r] = \mathbf{Z}/p^r\mathbf{Z}$

for some $r \geq 1$ (hence for all $r \geq 1$), and *E is supersingular at p* (or *p is a supersingular prime of E*) otherwise.

The torsion subgroup is more than just an abstract group; it has a structure of G_K-module. As G_K acts on each groups $E[m]$ continuously, we have a continuous Galois representation

$$\overline{\rho_m} : G_K \longrightarrow \mathrm{Aut}(E[m]) \approx \mathrm{GL}_2(\mathbf{Z}/m\mathbf{Z}).$$

It is often convenient to consider all torsion groups $E[\ell^r]$ at once for a fixed prime ℓ. As the family $(E[\ell^r])_{r\geq 0}$ forms a projective system via homomorphisms $[\ell] : E[\ell^{r+1}] \longrightarrow E[\ell^r]$ for each $r \geq 0$, we can take the limit,

$$T_\ell E := \varprojlim E[\ell^r].$$

This Galois module is called the *ℓ-adic Tate module attached to E*. If $\mathrm{char}(K) \neq \ell$, then $T_\ell E \approx \mathbf{Z}_\ell \oplus \mathbf{Z}_\ell$ as abstract groups. Furthermore, we let

$$V_\ell E := T_\ell E \otimes \mathbf{Q} \approx \mathbf{Q}_\ell \oplus \mathbf{Q}_\ell.$$

The resulting Galois representations

$$\rho_\ell : G_K \longrightarrow \mathrm{Aut}(T_\ell E) \approx \mathrm{GL}_2(\mathbf{Z}_\ell), \text{ or}$$
$$\rho_\ell : G_K \longrightarrow \mathrm{Aut}(V_\ell E) \approx \mathrm{GL}_2(\mathbf{Q}_\ell)$$

are called the *ℓ-adic Galois representation attached to E*. The following theorem is important for further investigation of this representation.

Theorem 2.6. *The determinant* $\det \rho_\ell$ *of the representation ρ_ℓ is equal to the* ℓ-adic cyclotomic character χ_ℓ, *which is the character $G_K \longrightarrow \mathrm{Aut}(\mathbf{Z}_\ell) = \mathbf{G}_m(\mathbf{Z}_\ell) \approx \mathbf{Z}_\ell^\times$ defined by $\sigma \longmapsto (a_r)_{r\geq 1}$ with $\sigma(\zeta_{\ell^r}) = \zeta_{\ell^r}^{a_r}$ for $a_r \in (\mathbf{Z}/\ell^r\mathbf{Z})^\times$, where (ζ_{ℓ^r}) is a system of ℓ-th power roots of unity chosen compatibly.*

The K-rational torsion subgroup of E/K is the subgroup of E_{tors} consisting of K-rational elements, i.e., elements fixed by the action of G_K. we denote this subgroup by $E(K)_{\mathrm{tors}}$. At least when $K = \mathbf{Q}$, finding the points in $E(\mathbf{Q})_{\mathrm{tors}}$ is relatively easy, provided the following theorem.

Theorem 2.7 (Lutz–Nagell)**.** *Let $E/\mathbf{Q}$ be an elliptic curve defined by Weierstrass equation*

$$y^2 = x^3 + Ax + B, \qquad A, B \in \mathbf{Z}. \tag{2.3}$$

If $P \in E(\mathbf{Q})$ is a nontrivial torsion point, then its x- and y- coordinates $x(P)$ and $y(P)$ are integers. Furthermore, we have either $[2]P = O$ or else $y(P)^2$ divides $4A^3 + 27B^2$.

Proof. Corollary VIII.7.2 in [Sil09]. □

Remark. If $\operatorname{char} K \neq 2, 3$, then all elliptic curves E over K has Weierstrass equation of the form in Equation (2.3). More precicely, given general Weierstrass equation (2.2), via change of variables

$$(x, y) \longmapsto \left(x, \frac{1}{2}(y - a_1x - a_3)\right) =: (x', y') \longmapsto \left(\frac{x' - 3b_2}{36}, \frac{y'}{108}\right),$$

we get another Weierstrass equation of the form

$$y^2 = x^3 - 27c_4x - 54c_6.$$

Classifying all rational torsion subgroup $E(\mathbf{Q})_{\text{tors}}$ for elliptic curves $E/\mathbf{Q}$ was an interesting problem. The following was a conjecture of Ogg, and proved by Mazur in 1970's.

Theorem 2.8 ([Maz78], Theorem 2)**.** *Let $E/\mathbf{Q}$ be an elliptic curve. Then the rational torsion subgroup $E(\mathbf{Q})_{\text{tors}}$ is isomorphic to one of the following 15 groups:*

$$\begin{aligned} \mathbf{Z}/m\mathbf{Z} \qquad & 1 \leq m \leq 10, \text{ or } m = 12, \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\nu\mathbf{Z} \qquad & 1 \leq \nu \leq 4. \end{aligned}$$

Moreover, given a group G which is one of the Mazur's 15 groups, we can parametrise the equations of the elliptic curves over $\mathbf{Q}$ having rational torsion subgroup G. This is one of the starting point of our research on Gross–Zagier theorem (see chapter 4). We refer to Table 3 in [Kub].

Other than $\mathbf{Q}$, the quadratic fields are the only cases in which we fully understand the torsion subgroups of elliptic curves.

Theorem 2.9 (Kamienny–Kenku–Momose)**.** *Let E be an elliptic curve defined over a quadratic field K. Then $E(K)_{\mathrm{tors}}$ is isomorphic to one of the following 26 groups:*

$$\begin{aligned} \mathbf{Z}/m\mathbf{Z} \qquad & 1 \le m \le 16, \text{ or } m = 18, \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\nu\mathbf{Z} \qquad & 1 \le \nu \le 6, \\ \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\nu\mathbf{Z} \qquad & 1 \le \nu \le 2, \\ \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}. & \end{aligned}$$

The above list of groups was proposed in [KeMo], and in 1992, Kamienny proved the list is complete ([Kam]).

2.4 Elliptic curves over local fields and reduction

Let K be a non-archimedean complete local field with normalised valuation $v : K^\times \longrightarrow \mathbf{Z}$, with the ring of integers O. The maximal ideal of O is denoted by $\mathfrak{p}$, and let k be the residue field $O/\mathfrak{p}$.

Let E/K be an elliptic curve defined by the Weierstrass equation of the form (2.2), i.e., coefficients a_i are in K. The equation is called *minimal* if $a_i \in O$ for all i and $v(\Delta)$ is minimal among all such Weierstrass equations defining E. In this section we assume E is given by a minimal Weierstrass equation. In this case we say Δ is a *minimal discriminant* of E.

The *reduction of E modulo $\mathfrak{p}$* is the curve $\widetilde{E}$ over k defined by the equation

$$y^2 + \widetilde{a_1}xy + \widetilde{a_3}y = x^3 + \widetilde{a_2}x^2 + \widetilde{a_4}x + \widetilde{a_6},$$

where $\widetilde{a_i} = a_i \mod \mathfrak{p}$. This curve is not necessarily an elliptic curve; it may have a singular point. Note that in any case $\widetilde{E}$ has at most one singular point. The following types appear when we reduce E modulo $\mathfrak{p}$.

- E has *good* reduction if $\widetilde{E}$ is nonsingular. This is equivalent to $v(\Delta) = 0$, i.e., $\widetilde{\Delta} \in k^\times$.

- E has *multiplicative* reduction if $\widetilde{E}$ has a nodal singularity.
- E has *additive* reduction if $\widetilde{E}$ has a cuspidal singularity.

When E has multiplicative reduction, we say E has *split* multiplicative reduction if the tangent directions at the singular point of $\widetilde{E}$ are defined over k, otherwise we say E has *non-split* multiplicative reduction. In this latter case the tangent lines are defined over a quadratic extension of k. We also say E has *semi-stable reduction* if E has good or multiplicative reduction.

These terminologies (multiplicative, additive) coincide with the group structure of the non-singular part $\widetilde{E}^{\mathrm{ns}}$ of $\widetilde{E}$:

- E has split multiplicative reduction if and only if $\widetilde{E}^{\mathrm{ns}} \cong \mathbf{G}_m$, the multiplicative group scheme over k,
- E has non-split multiplicative reduction such that the tangent directions at the singular point are defined over $k(\sqrt{d})$ if and only if $\widetilde{E}^{\mathrm{ns}} \cong \mathbf{G}_m[d]$, the twisted multiplicative group scheme over k,
- E has additive reduction if and only if $\widetilde{E}^{\mathrm{ns}} \cong \mathbf{G}_a$, the additive group scheme over k.

For details, see §II.3 in [Mil06].

The notion of reduction provides us a useful tool to study the nature of elliptic curves over local fields. Let an embedding $E \longrightarrow \mathbf{P}^2$ be given and let $P \in E(K)$ be a point. If we write $P = [x_0, y_0, z_0]$, then the reduced point $\widetilde{P} = [\widetilde{x_0}, \widetilde{y_0}, \widetilde{z_0}]$ is a point in $\widetilde{E}(k)$. This allows us to define the reduction map $r : E(K) \longrightarrow \widetilde{E}(k)$, which gives the following filtration on the group $E(K)$.

$$E^0(K) = \left\{P \in E(K) : r(P) = \widetilde{P} \in \widetilde{E}^{\mathrm{ns}}(k)\right\} = r^{-1}\left(\widetilde{E}^{\mathrm{ns}}(k)\right),$$
$$E^1(K) = \left\{P \in E^0(K) : r(P) = \widetilde{O}\right\} = r^{-1}(\widetilde{O}).$$

In fact, the homomorphism $E^0(K) \longrightarrow \widetilde{E}^{\mathrm{ns}}(k)$ is surjective with kernel $E^1(K)$.[2] The quotient $E(K)/E^0(K)$ is of special interest to us. This group is

[2]For proof, see Proposition VII.2.1 in [Sil09].

finite, and the following theorem says something about the structure of this group.

Theorem 2.10 (Néron–Tate)**.** *Let E/K be an elliptic curve. If E has split multiplicative reduction, then $E(K)/E^0(K)$ is a cyclic group of order $v(\Delta) = -v(j)$. In all other cases, the group $E(K)/E^0(K)$ is finite of order at most 4.*

Proof. This follows from Tate's algorithm. See the following section. For details see §IV.9 in [Sil94] or Tate's original article [Tat75]. □

Definition. The index $C = [E(K) : E^0(K)]$ is called the *Tamagawa number* of E/K. When E is defined over a global field K, then we denote by $C_\mathfrak{p}$ the *local Tamagawa number* $[E(K_\mathfrak{p}) : E^0(K_\mathfrak{p})]$ in order to distinguish Tamagawa numbers for various completions.

Sometimes the following criterion for determining good reduction is very useful. Let $I_K = I_\mathfrak{p}$ be the inertia subgroup of G_K. A G_K-module M is said to be *unramified* if I_K acts trivially on M.

Theorem 2.11 (Criterion of Néron–Ogg–Shafarevich)**.** *The following are equivalent.*

(i) *E has good reduction.*

(ii) *$E[m]$ is unramified for all m relatively prime to* $\mathrm{char}(k)$.

(iii) *$E[m]$ is unramified for infinitely many m relatively prime to* $\mathrm{char}(k)$.

(iv) *$T_\ell E$ is unramified for all $\ell \neq \mathrm{char}(k)$.*

(v) *$T_\ell E$ is unramified for some $\ell \neq \mathrm{char}(k)$.*

Proof. Theorem VII.7.1 in [Sil09]. □

The technique of reduction can be also used to determine torsion points. Along with Lutz–Nagell theorem (Theorem 2.7) the following result is also of frequent use.

Theorem 2.12. *Let E be an elliptic curve over a number field K, and let $\mathfrak{p}$ be a prime of K at which E has good reduction, and let k be the residue field of $\mathfrak{p}$, of characteristic p. Then for any $m \geq 1$ with $p \nmid m$, the reduction map $E(K)[m] \longrightarrow \widetilde{E}(k)$ is injective.*

Proof. Proposition VII.3.1 in [Sil09]. □

For general number fields K and for elliptic curves E/K, we can also adopt the notion of minimal equation of E/K. Let $\mathcal{O}$ be the ring of integers of K. A Weierstrass equation (2.2) defining E/K is called *minimal* if $a_i \in \mathcal{O}$ and $v_{\mathfrak{p}}(\Delta)$ is minimal among all such equations, for every prime $\mathfrak{p}$ of K. However, global minimal equations do not always exist; but we are content with the following criterion.

Theorem 2.13. *K has class number 1 if and only if every elliptic curve E/K has a global minimal Weierstrass equation. In particular, every elliptic curve over $\mathbf{Q}$ has a global minimal equation.*

Proof. Corollary VIII.8.3 and Exercise 8.14 in [Sil09]. □

2.5 Néron models and Tate's algorithm

Let K be a complete local field. In this section however, more specifically, let K be a finite extension of p-adic number field $\mathbf{Q}_p$, and let $\mathfrak{p}$ be the prime of K lying above p. Moreover, let $\mathcal{O}$ be the ring of integers in K, and $k = \mathcal{O}/\mathfrak{p}$ be the residue field. In this section we use terminologies and concepts from modern (Grothendieck style) algebraic geometry more heavily. For definitions and relevant properties of such concepts, we refer to [Har], [Liu], or [Mum].

Suppose that E_K is an elliptic curve defined over K. As we have seen in the last section, one of the most useful tool to study the arithmetic of E_K is the method of reduction. If E_K is given by a minimal Weierstrass equation, then the coefficients a_i in Equation (2.1) are in $\mathcal{O}$, and so the equation defines

a projective scheme $W = W_{\mathcal{O}} \longrightarrow \operatorname{Spec} \mathcal{O}$, called the minimal Weierstrass model for E_K. When E_K has good reduction, this scheme is smooth (i.e., it is flat and locally of finite presentation over its base such that all fibres are geometrically regular; for precise definition, consult §II.2 in [BLR]) proper group scheme, so that E_K extends to an abelian scheme $W \longrightarrow \operatorname{Spec} \mathcal{O}$. However, when E_K has bad reduction, it is no longer true. Number theorists were interested to know whether such "good models" exist when E_K does not have good reduction. In 1960's, Néron discovered such good models do exist:

> "It came as a surprise for arithmeticians and algebraic geometers when A. Néron, relaxing the condition of properness and concentrating on the group structure and the smoothness, discovered in the years 1961–1963 that such models exist in a canonical way (...)"[3]

Let us now define the canoncial model of Néron.

Definition. Let E_K be an elliptic curve defined over K. A *Néron model for* E_K is a smooth group scheme $E = E_{\mathcal{O}}/\mathcal{O}$ whose generic fibre is E_K and which satisfies the following universal property, called *Néron mapping property*:

> Let $X/\mathcal{O}$ be any smooth group scheme over $\mathcal{O}$ with generic fibre X_K/K, and let $\phi_K : X_K \dashrightarrow E_K$ be a rational map defined over K. Then there exists a unique morphism $\phi : X \longrightarrow E$ defined over $\mathcal{O}$ extending ϕ_K.

Equivalently, the Néron mapping property says that the canonical injection $E(\mathcal{O}) = \operatorname{Mor}(\operatorname{Spec} \mathcal{O}, E) \longrightarrow E_K(K) = \operatorname{Mor}(\operatorname{Spec} K, E_K)$ is bijective.

Néron models can be defined more generally for abelian varieties A_K.

[3] [BLR], page 1.

Theorem 2.14 (Néron). *Let A_K be an abelian variety. Then the Néron model $A_{\mathcal{O}}$ exists and are unique up to a unique isomoprhism.*

Proof. See [Art]. □

One major problem is to determine which geometric structure appears in the special fibre of a Néron model $E/\mathcal{O}$ with generic fibre E_K/K. Let $E_k = E \times_{\operatorname{Spec}\mathcal{O}} \operatorname{Spec} k$ be the special fibre of E, and let E_k^0/k be the identity component of E_k. Note that a section $s \in E(\mathcal{O})$ which is the map $s : \operatorname{Spec}\mathcal{O} \longrightarrow E$ gives via composition with $\operatorname{Spec} k \longrightarrow \operatorname{Spec}\mathcal{O}$ that a point $(s, \mathrm{id}_k) : \operatorname{Spec} k \longrightarrow E \times_{\operatorname{Spec}\mathcal{O}} \operatorname{Spec} k = E_k$. As soon as we identify $E_K(K) \cong E(\mathcal{O})$, we restore the reduction map $r : E_K(K) \longrightarrow E_k(k)$. Then we have

$$E_k^0(k) \cong \widetilde{E_K}^{\mathrm{ns}}(k) \cong E_K^0(K)/E_K^1(K) \text{ and}$$
$$E_k(k)/E_k^0(k) \cong E_K(K)/E_K^0(K).$$

This allows us another description of the quotient group $E_K(K)/E_K^0(K)$, and it sheds some light on computing, in particular, the Tamagawa number $[E_K(K) : E_K^0(K)]$.

In order to determine the special fibre, we need to consider more geometrically. So, let $C/\operatorname{Spec}\mathcal{O}$ be the *minimal regular proper model of* E_K, by which we mean a proper flat $\mathcal{O}$-model C which is a regular scheme and which is minimal among all models C' of this type, such that its generic fibre $C_K = C \times_{\operatorname{Spec}\mathcal{O}} \operatorname{Spec} K$ is isomorphic over K to E_K. Here by the minimality we mean that each $\mathcal{O}$-morphism $C \longrightarrow C'$ of such models which becomes isomorphic on the generic fibre is in fact an isomorphism. Such models uniquely exist; for detail, we refer to [Abh], [Lip] or [Nér]. The Néron model E for E_K is in fact obtained from C by removing all the singular points of the special fibre $C_k = C \times_{\operatorname{Spec}\mathcal{O}} \operatorname{Spec} k$. Néron actually classified all geometric structures that can appear as special fibre of C: in Kodaira's notation ([Kod64], [Kod66]), they are I_0 (good reduction), I_n for $n \geq 1$ (multiplicative reduction), II, III, IV I_0^*, I_n^* for $n \geq 1$, II*, III*, and IV*.

When an elliptic curve E_K/K is given, Tate's algorithm determines the exact Kodaira type of the special fibre, together with the number of geometric components, the valuation of the minimal discriminant, the exponent of the conductor of E_K (which will be defined soon), and finally, the Tamagawa number $C = [E_K(K) : E_K^0(K)]$. Writing down Tate's algorithm here is too lengthy and somewhat redundant, we are content ourselves with refering to §IV.9 in [Sil94] and Tate's original article [Tat75].

Before closing this section, we define an arithmetic invariant (in fact, isogeny-invariant) of elliptic curves E defined over a number field K that contains the informations about the local reduction types of E.

Definition. Let E be an elliptic curve defined over a number field K. The *conductor of* E/K is the product

$$N = \prod_{\mathfrak{p}} \mathfrak{p}^{f_\mathfrak{p}},$$

where the product runs over all finite primes of K, and $f_\mathfrak{p}$ is an integer defined by

$$f_\mathfrak{p} = \begin{cases} 0 & \text{if } E/K \text{ has good reduction at } \mathfrak{p}, \\ 1 & \text{if } E/K \text{ has multiplicative reduction at } \mathfrak{p}, \\ 2 + \delta_\mathfrak{p} & \text{if } E/K \text{ has additive reduction at } \mathfrak{p}. \end{cases}$$

When E/K has additive reduction at $\mathfrak{p}$, the quantity $\delta_\mathfrak{p} \geq 0$ is called the *wild part of the conductor of* E/K *at* $\mathfrak{p}$.

Remark. The wild part of the conductor E/K at $\mathfrak{p}$ is annoying, but mostly harmless because $\delta_\mathfrak{p} = 0$ for all $p \geq 5$, where p is the residue characteristic of $K_\mathfrak{p}$. Of course we have rigorous definition for $\delta_\mathfrak{p}$, which can be found at §IV.10 of [Sil94]. Moreover, for any $\mathfrak{p}$, the wild part $\delta_\mathfrak{p}$ is completely computable by Tate's algorithm.

Remark. At first, one could think of the conductor as a quite redundant quantity because of the existence of the minimal discriminant. But in fact it is never an *ad hoc* invariant; it is relevant to Galois representation attached to elliptic curves, and plays a very important role in the functional equation of the L-function.

2.6 Elliptic curves over number fields and Mordell–Weil theorem

Let K be a number field, and O be the ring of integers of K. The following is arguably the most important theorem on the arithmetic of elliptic curves; it describes the structure of the group of rational points $E(K)$.

Theorem 2.15 (Mordell–Weil)**.** *Let E be an elliptic curve over K. Then the group $E(K)$ is finitely generated abelian group, i.e., we can write*

$$E(K) \cong \mathbf{Z}^r \oplus E(K)_{\text{tors}},$$

where $r = r_E \geq 0$ is an integer called the rank of E/K*, and $E(K)_{\text{tors}}$ is a finite abelian group.*

We sketch the proof of the theorem. Basically, the proof consists of two parts: weak Mordell–Weil theorem and height consideration. Throughout this section, we closely follow expositions on the text of Hindry and Silverman, [HiSi], especially chapter C in the text.

The weak Mordell–Weil theorem says that for each integer $m \geq 1$, the quotient group $E(K)/mE(K)$ is finite. In order to see this, we consider a more general situation; let $\phi : E \longrightarrow E'$ be an isogeny, and we will see that the quotient $E'(K)/\phi E(K)$ is finite. Let $E[\phi] = E(\overline{K})[\phi]$ be its kernel. Then we have the following short exact sequence of G_K-modules which is analogous to the classical Kummer sequence (cf. §X.3 in [Ser79]):

$$0 \longrightarrow E(\overline{K})[\phi] \longrightarrow E(\overline{K}) \xrightarrow{\phi} E'(\overline{K}) \longrightarrow 0.$$

By taking the cohomology long exact sequence, we get

$$0 \longrightarrow E(K)[\phi] \longrightarrow E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(K, E[\phi]) \longrightarrow H^1(K, E) \xrightarrow{\phi} H^1(K, E') \longrightarrow \cdots,$$

where δ is the connecting homomorphism. From this, we can extract the following short exact sequence:

$$0 \longrightarrow E'(K)/\phi E(K) \longrightarrow H^1(K, E[\phi]) \longrightarrow H^1(K, E)[\phi] \longrightarrow 0.$$

So in order to show the finiteness of $E'(K)/\phi E(K)$, it is sufficient to obtain the finiteness of $H^1(K, E[\phi])$. However, unfortunately, the latter group is almost always infinite; we avoid this difficulty by finding a finite subgroup of $H^1(K, E[\phi])$ containing $E'(K)/\phi E(K)$. We find such a group by considering completions with respect to various primes of K. So let $\mathfrak{p}$ be a prime of K, and let $K_\mathfrak{p}$ be the completion of K with respect to $\mathfrak{p}$, which is a complete local field with valuation $v = v_\mathfrak{p}$. Let M be an arbitrary continuous G_K-module. If we fix an extension of v in $\overline{K}$, i.e., an embedding $\overline{K} \longrightarrow \overline{K_\mathfrak{p}}$ for each prime $\mathfrak{p}$, then the local absolute Galois groups $G_\mathfrak{p} := \mathrm{Gal}(\overline{K_\mathfrak{p}}/K_\mathfrak{p})$ are embedded in G_K as decompostion groups. These embeddings give restriction maps on cohomology groups:

$$\mathrm{res}_\mathfrak{p} : H^q(K, M) \longrightarrow H^q(K_\mathfrak{p}, M) \qquad q \geq 0.$$

Thus, we have the following diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E'(K)/\phi E(K) & \longrightarrow & H^1(K, E[\phi]) & \longrightarrow & H^1(K, E)[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod_\mathfrak{p} E'(K_\mathfrak{p})/\phi E(K_\mathfrak{p}) & \longrightarrow & \prod_\mathfrak{p} H^1(K_\mathfrak{p}, E[\phi]) & \longrightarrow & \prod_\mathfrak{p} H^1(K_\mathfrak{p}, E)[\phi] & \longrightarrow & 0
\end{array}$$

where the vertical maps are restriction maps.

Definition. Let $\phi : E \longrightarrow E'$ be an isogeny of elliptic curves defined over a number field K. The *Selmer group of E with respect to ϕ* (or *ϕ-Selmer group* for short) is the group

$$\mathrm{Sel}^{\phi}(E/K) := \ker\left(H^1(K, E[\phi]) \longrightarrow \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, E)[\phi]\right).$$

The *Tate–Shafarevich group of E* is the group

$$Ш(E/K) := \ker\left(H^1(K, E) \longrightarrow \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, E)\right).$$

In both formulae, the product is taken over all (finite and infinite) primes $\mathfrak{p}$ of K.

Remark. Note that there are some variations on the definitions of the Selmer and Tate–Shafarevich groups. For example, we have

$$\begin{aligned}\mathrm{Sel}^{\phi}(E/K) &= \bigcap_{\mathfrak{p}} \ker\left(H^1(K, E[\phi]) \longrightarrow H^1(K_{\mathfrak{p}}, E)[\phi]\right) \text{ or} \\ &= \left\{\xi \in H^1(K, E[\phi]) : \mathrm{res}_{\mathfrak{p}}\, \xi \in \mathrm{im}\, \delta_{\mathfrak{p}}\right\},\end{aligned}$$

where $\delta_{\mathfrak{p}} : E'(K_{\mathfrak{p}}) \longrightarrow H^1(K_{\mathfrak{p}}, E[\phi])$ is the connecting homomorphism for each prime $\mathfrak{p}$. In fact, this last expression is useful later for computing Selmer groups.

Now, using these new groups, we have the following exact sequence

$$0 \longrightarrow E'(K)/\phi E(K) \longrightarrow \mathrm{Sel}^{\phi}(E/K) \longrightarrow Ш(E/K)[\phi] \longrightarrow 0.$$

Theorem 2.16. *The ϕ-Selmer group $\mathrm{Sel}^{\phi}(E/K)$ is finite. Consequently, the subgroups $E'(K)/\phi E(K)$ and $Ш(E/K)[\phi]$ are also finite.*

Our strategy to prove finiteness of $\mathrm{Sel}^{\phi}(E/K)$ is, again, to embed the group into another finite group we are able to deal with more easily. Let M be a continuous G_K-module. For a prime $\mathfrak{p}$ of K, we say a cohomology class $\xi \in H^1(K, M)$ is *unramified* at $\mathfrak{p}$ if its restriction to $H^1(I_{\mathfrak{p}}, M)$ is trivial, where $I_{\mathfrak{p}} \subset G_{\mathfrak{p}}$ is an inertia group for $\mathfrak{p}$. Note that $I_{\mathfrak{p}}$ is only defined up to conjugation since the choice of extension of $\mathfrak{p}$ matters, but the triviality or non-triviality of the image of ξ via the restriction maps is not dependent on the choice of $I_{\mathfrak{p}}$. Having defined that, for a finite set S of primes

of K, we denote by $H^1_S(K, M)$ the subgroup of $H^1(K, M)$ consisting of cohomology classes that are unramified outside S. The theorem now follows from the following two lemmas.

Lemma 2.17. *Let M be a finite continuous G_K-module, and let S be a finte set of primes of K. Then the cohomology group $H^1_S(K, M)$ of classes unramified outside S is finite.*

Proof. Since M is finite and G_K acts continuously on M, we can take a finite Galois extension L/K such that $G_L \subset G_K$ acts trivially on M. From the inflation-restiction sequence

$$0 \longrightarrow H^1(\mathrm{Gal}(L/K), M^{\mathrm{Gal}(L/K)}) \xrightarrow{\inf} H^1(K, M) \xrightarrow{\mathrm{res}} H^1(L, M),$$

it follows that we are reduced to prove the result for L. Replacing K by L, we assume G_K acts trivially on M. Let m be the exponent of the abelian group M.

Now, the elements of $H^1(K, M) = \mathrm{Hom}(G_K, M)$ correspond to certain finite abelian extensions whose Galois groups have exponent m; when $\xi \in \mathrm{Hom}(G_K, M)$ is given, then the field $\overline{K}^{\ker \xi}$ is the desired finite abelian extension of K. Via this correspondance, elements of $H^1_S(K, M)$ corresponds to finite abelian extensions of exponent m unramified outside S. By Kummer theory we can see that the maximal abelian extension of K of exponent m is finite (see Corollary C.1.8 in [HiSi]); we deduce $H^1_S(K, M)$ is also finite. □

Lemma 2.18. *Let $\phi : E \longrightarrow E'$ be an isogeny of elliptic curves over K. Let S be a finite set of primes of K containing*

(i) all infinite primes of K,

(ii) all primes of bad reduction of E and E' (in fact E and E' have the same set of primes of bad reduction[4]),

(iii) all primes dividing the degree of ϕ.

Then one can embed $\mathrm{Sel}^{\phi}(E/K)$ *into* $H^1_S(K, E[\phi])$.

[4]This is due to the criterion of Néron–Ogg–Shafarevich. See Theorem 2.11.

Proof. Let $\xi \in \mathrm{Sel}^{\phi}(E/K) \subset H^1(K, E[\phi])$ and let $\mathfrak{p}$ be a finite prime not in S. By the definition of $\mathrm{Sel}^{\phi}(E/K)$ we can choose a point $x \in E(\overline{K_{\mathfrak{p}}})$ such that $\mathrm{res}_{\mathfrak{p}}\, \xi(\sigma) = \sigma(x) - x$ for each $\sigma \in G_{\mathfrak{p}}$. Suppose that $\sigma \in I_{\mathfrak{p}}$. Since any elements of $I_{\mathfrak{p}}$ acts trivially on $\widetilde{E}(\overline{k_{\mathfrak{p}}})$ where $k_{\mathfrak{p}}$ is the residue field at the prime $\mathfrak{p}$, we have

$$\xi(\sigma) = \sigma(x) - x \equiv 0 \pmod{\mathfrak{p}}.$$

However, since $\sigma(x) - x \in E[\phi] \subset E[m]$ for $m = \deg \phi$ and m is relatively prime to $\mathfrak{p}$, by Theorem 2.12, we must have $\xi(\sigma) = \sigma(x) - x = 0$, whence $\mathrm{Sel}^{\phi}(E/K) \subset H^1_S(K, E[\phi])$. □

We have proved Theorem 2.16. Applying the theorem to the case when $E = E'$ and $\phi = [m]$, we get the weak Mordell–Weil theorem for m: the group $E(K)/mE(K)$ is finite.

The second step towards Mordell–Weil theorem (Theorem 2.15) makes use of height functions. So let us introduce briefly about the height functions and complete the proof of Theorem 2.15. Height functions are defined gradually from height functions on projective spaces to ones on elliptic curves.

We first need to fix our notion of absolute values. Let $M_{\mathbf{Q}} = M^{\infty}_{\mathbf{Q}} \cup M^{0}_{\mathbf{Q}}$ be the *set of standard absolute values on* $\mathbf{Q}$. Furthermore,

- $M^{\infty}_{\mathbf{Q}}$ is a singleton containing the archimedean absolute value $|\cdot|_{\infty}$ on $\mathbf{Q}$, i.e., $|x|_{\infty} = \max(x, -x)$, and
- $M^{0}_{\mathbf{Q}}$ is the set of p-adic absolute values $|\cdot|_p$ for rational primes p, i.e., $|x|_p = p^{-\mathrm{ord}_p\, x}$.

Let K be a number field, i.e. $K/\mathbf{Q}$ is a finte algebraic extension. Then the *set of standard absolute values on* K, denoted by M_K is defined as the set of all absolute values on K, whose restriction to $\mathbf{Q}$ is one of the absolute values in $M_{\mathbf{Q}}$.

Definition. Let $\mathbf{P}^N$ be the projective space of dimension N, defined over $\mathbf{Q}$.

(i) The *(naïve) multiplicative height function relative to* K is the function $H_K : \mathbf{P}^N(K) \longrightarrow \mathbf{R}$ defined by

$$P = [x_0, \cdots, x_N] \longmapsto H_K(P) = \prod_{\mathfrak{p}} \max\left(|x_0|_{\mathfrak{p}}, \cdots, |x_N|_{\mathfrak{p}}\right)^{n_{\mathfrak{p}}},$$

where the product is taken over all primes of K, and $n_{\mathfrak{p}}$ is the local degree at $\mathfrak{p}$, i.e., $n_{\mathfrak{p}} = [K_{\mathfrak{p}} : \mathbf{Q}_p]$ for p being the rational prime lying below $\mathfrak{p}$.

(ii) If $P \in \mathbf{P}^N(\overline{\mathbf{Q}})$, then we define the *multiplicative absolute height of* P, denoted by $H(P)$ as follows. We first choose a number field K such that $P \in \mathbf{P}^N(K)$. Then $H(P) = H_K(P)^{1/[K:\mathbf{Q}]}$.

(iii) The *absolute (logarithmic) height* is the function $h : \mathbf{P}^N(\overline{\mathbf{Q}}) \longrightarrow \mathbf{R}$ defined by $h(P) = \log H(P)$.

The multiplicative height is well-defined by the product formula (see §III.1 in [Neu99] for example). Moreover, we have $H_K(P) \geq 1$ for all number field K and $P \in \mathbf{P}^N(K)$, whence $h(P) \geq 0$.

Now let E/K be an elliptic curve, and let $f \in \overline{K}(E)$ be a non-constant function. Then f defines a surjective morphism which is also denoted by f,

$$f : E \longrightarrow \mathbf{P}^1, \qquad P \longmapsto \begin{cases} [1,0] & \text{if } P \text{ is a pole of } f, \\ [f(P),1] & \text{otherwise.} \end{cases}$$

Definition. The *height on E relative to f* is the function

$$h_f : E \longrightarrow \mathbf{R}, \qquad P \longmapsto h(f(P)).$$

We use the following property.

Proposition 2.19. *Let E/K be an elliptic curve and let $f \in K(E)$ be a non-constant function defined over K.*

(i) For any constant C, the set

$$\left\{P \in E(K) : h_f(P) \leq C\right\}$$

is finite.

(ii) Let $Q \in E(\overline{K})$. Then

$$h_f(P+Q) \leq 2h_f(P) + O(1) \quad \text{for all } P \in E(\overline{K}),$$

where $O(1)$ depends on E, f and Q.

(iii) Let $m \in \mathbf{Z}$. Then

$$h_f([m]P) = m^2 h_f(P) + O(1) \quad \text{for all } P \in E(\overline{K}),$$

where $O(1)$ depends on E, f, and m.

Proof. Proposition VIII.6.1 through Corollary VIII.6.4 in [Sil09]. □

Now we prove Theorem 2.15. We follow the proof of Theorem VIII.3.1 and Theorem VIII.6.7 in [Sil09].

Proof of Mordell–Weil Theorem. Choose any function $f \in K(E)$, for example, f could be the x-coordinate on a Weierstrass equation for E, and denote by $h = h_f$ the height on E relative to f. Fix an integer $m \geq 2$, and choose elements $Q_1, \cdots, Q_r \in E(K)$ representing the finitely many cosets in $E(K)/mE(K)$. Let $P \in E(K)$ be an arbitrary element, then we can find Q_{i_1} $(1 \leq i_1 \leq r)$ representing the coset $P + mE(K)$, i.e., $P = [m]P_1 + Q_{i_1}$ for some $P_1 \in E(K)$. Similarly, write

$$\begin{aligned} P &= [m]P_1 + Q_{i_1}, \\ P_1 &= [m]P_2 + Q_{i_2}, \\ &\cdots \\ P_{n-1} &= [m]P_n + Q_{i_n}. \end{aligned}$$

For each index j, we have

$$\begin{aligned} h(P_j) &= \frac{1}{m^2}\left(h([m]P_j) + C\right) && \text{from (iii) of Proposition 2.19,} \\ &= \frac{1}{m^2}\left(h(P_{j-1} - Q_{i_j}) + C\right) \\ &\leq \frac{1}{m^2}\left(2h(P_{j-1}) + C'\right) && \text{from (ii) of Proposition 2.19.} \end{aligned}$$

Here, as f and m being fixed, the constant C' only depends on E, by choosing maximal constant of Proposition 2.19 (ii) for $Q \in \{-Q_1, \cdots, -Q_r\}$. Applying this

inequality repeatedly, we have

$$\begin{aligned} h(P_n) &\leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^2} + \frac{4}{m^2} + \cdots + \frac{2^{n-1}}{m^2}\right) C' \\ &< \left(\frac{2}{m^2}\right)^n h(P) + \frac{C'}{m^2 - 2} \\ &\leq \left(\frac{2}{m^2}\right)^n h(P) + \frac{C'}{2}. \end{aligned}$$

The last inequality holds because $m \geq 2$. Thus, for sufficiently large n, we have $h(P_n) \leq 1 + \dfrac{C'}{2}$. Since

$$P = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j},$$

we conclude that any point $P \in E(K)$ is a linear combination of points in the set

$$\{Q_1, \cdots, Q_r\} \bigcup \left\{ Q \in E(K) : h(Q) \leq 1 + \frac{C'}{2} \right\}.$$

From Proposition 2.19 (i), this set is finite, whence $E(K)$ is finitely generated. □

Among other things, Proposition 2.19 (iii) shows that the function h_f is "almost" a quadratic form. In fact, there is a quadratic form which only differ from h_f by a constant. The following is the construction of such quadratic form, which is due to Tate.

Proposition 2.20. *Let E/K be an elliptic curve and let $f \in K(E)$ be a non-constant* even *function. Then for each $P \in E(\overline{K})$, the limit*

$$\frac{1}{\deg f} \lim_{N \longrightarrow \infty} 4^{-N} h_f([2^N]P)$$

exists, and it is independent of f.

Proof. Proposition VIII.9.1 in [Sil09]. □

This allows us to define the following.

Definition. The *canonical (or Néron–Tate) height on E/K* is the function

$$\hat{h} : E(\overline{K}) \longrightarrow \mathbf{R}$$

defined by

$$\hat{h}(P) = \frac{1}{\deg f} \lim_{N \longrightarrow \infty} 4^{-N} h_f([2^N]P),$$

where f is any non-constant even function in $\overline{K}(E)$.

As we have mentioned, this function enjoys all the properties of the quadratic form.

Theorem 2.21 (Néron–Tate)**.** *Let E/K be an elliptic curve, and let $\hat{h}$ be the Néron–Tate height on E.*

(i) For all $P, Q \in E(\overline{K})$, we have

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q).$$

(ii) For all $P \in E(\overline{K})$ and all $m \in \mathbf{Z}$,

$$\hat{h}([m]P) = m^2 \hat{h}(P).$$

(iii) $\hat{h}$ is a quadratic form on E, i.e., $\hat{h}$ is an even function and the pairing

$$\langle \cdot, \cdot \rangle : E(\overline{K}) \times E(\overline{K}) \longrightarrow \mathbf{R}$$

defined by

$$\langle P, Q \rangle = \frac{1}{2} \left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q) \right)$$

is bilinear.

(iv) We have $\hat{h}(P) \geq 0$ for all P, and the equaility holds if and only if P is a torsion point.

(v) Let $f \in K(E)$ be an even function. Then

$$(\deg f)\hat{h} = h_f + O(1),$$

where $O(1)$ depends on E and f.

(vi) *If $\hat{h}' : E(\overline{K}) \longrightarrow \mathbf{R}$ is any other function saisfying (v) and (ii) for some integer $m \geq 2$, then $\hat{h}' = \hat{h}$.*

Proof. Theorem VIII.9.3 in [Sil09]. □

Intuitively, we regard $\hat{h}$ as the function measuring the arithmetic complexity of points on E. This gives an important invariant relative to the arithmetic of elliptic curves, as follows. We use the *canonical (or Néron–Tate) height pairing on E*, $\langle \cdot, \cdot \rangle$, defined above.

Definition. Let E/K be an elliptic curve, and let $\{P_1, \cdots, P_r\}$ be a basis of the free part $E(K)/E(K)_{\text{tors}}$. The *regulator of $E(K)$* is defined by

$$\text{Reg}(E/K) = \det\left(\langle P_i, P_j \rangle\right)_{1 \leq i,j \leq r}.$$

If $r = 0$, i.e., if $E(K)$ is finite, then we define $\text{Reg}(E/K) = 1$.

2.7 Hasse–Weil L-functions

We first define the L-series attached to the elliptic curve. It is defined as an Euler product, with the factors indexed by finite primes of K; the idea is to gather all local informations to form a meromorphic function defined initially on some half plane in $\mathbf{C}$.

Let E be an elliptic curve defined over a number field K. Let $\mathfrak{p}$ be a prime of K, and consider the completion $K_\mathfrak{p}$ of K with respect to $\mathfrak{p}$ and the corresponding decomposition group $G_\mathfrak{p}$. Let $k_\mathfrak{p} \approx \mathbf{F}_{q_\mathfrak{p}}$ be the finite residue field of $K_\mathfrak{p}$ with characteristic p. The group $G_\mathfrak{p}$ is determined up to conjugation, inside the full Galois group G_K. Once it is fixed, we can talk of Frobenius element $\text{Frob}_\mathfrak{p} \in G_\mathfrak{p}$ which is also determined up to inertia group $I_\mathfrak{p}$.

Let ℓ be a prime, and consider the Galois representations $T_\ell E$ and $V_\ell E = T_\ell E \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ of the group $G_\mathfrak{p}$, and its dual $V_\ell E^\vee$. Since the quotient $G_\mathfrak{p}/I_\mathfrak{p}$ acts on $(V_\ell E)^{I_\mathfrak{p}}$, the action of $\text{Frob}_\mathfrak{p}$ on it is well-defined. Moreover, since its characteristic polynomial is invariant under conjugation, the action of $\text{Frob}_\mathfrak{p}$ is completely well-defined. Now we define the local polynomial at $\mathfrak{p}$ as follows:

$$F_\mathfrak{p}(T) = \det\left(1 - \text{Frob}_\mathfrak{p}^{-1}\, T | (V_\ell E^\vee)^{I_\mathfrak{p}}\right).$$

Here, using the inverse of Frobenius and dual of $V_\ell E$ is only conventional; we do not pay more attention to it.

Suppose first that E has good reduction at $\mathfrak{p}$. By the criterion of Néron–Ogg–Shafarevich (Theorem 2.11), it is true if and only if $V_\ell E$ is unramified at $\mathfrak{p}$. By properties of Frobenius actions on elliptic curves over finite fields (cf. chapter V in [Sil09]), we have

$$F_\mathfrak{p}(T) = 1 - a_\mathfrak{p} T + q_\mathfrak{p} T^2.$$

where

$$a_\mathfrak{p} = 1 + q_\mathfrak{p} - \#\widetilde{E}(k_\mathfrak{p}).$$

When E has bad reduction at $\mathfrak{p}$, we can also decide the local polynomials as follows (cf. §3 in [Dok]).

$$F_\mathfrak{p}(T) = \begin{cases} 1 & \text{if } E \text{ has additive reduction at } \mathfrak{p}, \\ 1 - T & \text{if } E \text{ has split multiplicative reduction at } \mathfrak{p}, \\ 1 + T & \text{if } E \text{ has non-split multiplicative reduction at } \mathfrak{p}. \end{cases}$$

Now we are ready to define the L-function.

Definition. The *Hasse–Weil L-function of* E/K (or the *L-function attached to the elliptic curve* E/K) is a function of a complex variable s given by the Euler factor

$$L(E/K, s) = \prod_\mathfrak{p} F_\mathfrak{p}(q_\mathfrak{p}^{-s})^{-1} = \prod_\mathfrak{p} \det\left(1 - q_\mathfrak{p}^{-s} \operatorname{Frob}_\mathfrak{p}^{-1} \,|\, (V_\ell E^\vee)^{I_\mathfrak{p}}\right)^{-1}, \tag{2.4}$$

where the product is taken over all finite primes of K.

Remark. The L-function of E/K is isogeny-invariant, i.e., if E and E' are isogenous curves over K, then $L(E/K, s) = L(E'/K, s)$. This comes from the nature of the above Euler product; the factors are actually defined in terms of Galois representation attached to E, and Faltings's isogeny theorem ([Fal]) shows that an isogeny $E \longrightarrow E'$ gives rise to an isomorphism $V_\ell E \longrightarrow V_\ell E'$ on Tate modules.

Theory of Hasse bound (§V.1 in [Sil09]) shows that the product in Equation (2.4) converges absolutely in the half plane $\operatorname{Re}(s) > 3/2$. Note that, however, *formal*

evaluation at $s = 1$ of Equation (2.4) gives

$$L(E/K, 1)\text{“}=\text{”} \prod_{\mathfrak{p}} \frac{q_{\mathfrak{p}}}{\#\widetilde{E}^{\mathrm{ns}}(k_{\mathfrak{p}})},$$

which inspires Birch and Swinnerton-Dyer to formulate the famous “BSD” conjecture. This will be dealt with in the subsequent section.

The prototype of the Hasse–Weil L-function, as of all objects in number theory called “L-functions” or “zeta functions”, is the *Riemann zeta function*. It is defined by $\zeta(s) = \sum_{n\geq 1} n^{-s}$, which is a Dirichlet series, or by the product of Euler factors

$$\zeta(s) = \prod_{p} (1 - p^{-s})^{-1},$$

where the product runs over all rational primes p. Note the similarity of appearances of the Riemann zeta and Hasse–Weil L-functions. The same moral is also applied for the Hasse–Weil L-function; namely the complex function formed by gathering all local informations mysteriously covers a lot of arithmetic invariants encoded at the critical points. This idea is also infiltrated into the BSD conjecture.

However, before getting into the BSD conjecture, we must overcome the following conjecture concerning about meromorphic continuation and functional equations of the L-function.

Conjecture 2.22 (Hasse–Weil)**.** Suppose that E is an elliptic curve of conductor N_E defined over a number field K. Let

$$\Lambda(E/K, s) := \left((2\pi)^{-s}\Gamma(s)\right)^{[K:\mathbf{Q}]} \cdot \left(\mathrm{Norm}_{K/\mathbf{Q}}(N_E)\right)^{s/2} \cdot (\mathrm{disc}\, K)^{s} \cdot L(E/K, s),$$

be the *completed L-function*, where $\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}dt$ is the Gamma function and $\mathrm{disc}(K)$ is the discriminant of K. The function $\Lambda(E/K, s)$ is understood as adding factors at the infinite primes to $L(E/K, s)$. Then,

$$\Lambda(E/K, s) = w(E/K)\Lambda(E/K, 2 - s), \tag{2.5}$$

where $w(E/K) = \pm 1$ is called the *root number of* E/K. In particular, this functional equation implies that the Euler product (2.4) defined on $\mathrm{Re}(s) > 3/2$ admits a meromorphic continuation to entire $\mathbf{C}$.

As of today, this conjecture is known for all elliptic curves over $K = \mathbf{Q}$; this is a formal consequence of Modularity Theorem, which was deliberately shown by Wiles ([Wil], with some correction [TaWi] with Taylor) for semi-stable elliptic curves, and by [BCDT] for all elliptic curves over $\mathbf{Q}$. Besides $\mathbf{Q}$, some other cases when K is totally real are known.

2.8 Modular curves and modularity theorem

In this section, we briefly review topics related to modular curves and modularity of elliptic curves over $\mathbf{Q}$. We will see that modularity theorem for elliptic curves over $\mathbf{Q}$ implies the Hasse–Weil conjecture (Conjecture 2.22).

Let $N \geq 1$ be an integer, and let

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : c \equiv 0 \pmod{N} \right\},$$

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : c \equiv 0,\ a \equiv d \equiv 1 \pmod{N} \right\}$$

be congruence subgroups of $\mathrm{SL}_2(\mathbf{Z})$. Note that any elements of $\mathrm{SL}_2(\mathbf{Z})$ acts on the extended Poincaré upper half plane

$$\mathfrak{H}^* = \{z \in \mathbf{C} : \mathrm{Im}\, z > 0\} \cup \mathbf{P}^1(\mathbf{Q}).$$

by linear fractional transformations (on the upper half plane) and by the obvious manner (on $\mathbf{P}^1(\mathbf{Q})$). Over $\mathbf{C}$, we define modular curves $X_0(N)_{\mathbf{C}}$ and $X_1(N)_{\mathbf{C}}$ by letting $X_i(N)_{\mathbf{C}} := \Gamma_i(N)\backslash\mathfrak{H}^*$ for $i = 0, 1$. Then $X_i(N)_{\mathbf{C}}$ are compact Riemann surfaces, or equivalently, complete algebraic curves.

In fact, we take models $X_i(N)$ for the Riemann surfaces $X_i(N)_{\mathbf{C}}$ defined over $\mathbf{Q}$; there are plenty of literatures on this topic, and we refer to e.g. [DDT], [DiIm] and [Roh]. From now on, we think of $X_i(N)$ as algebraic curves defined over $\mathbf{Q}$. This curves have nice properties as moduli spaces. First, the curve $X_0(N)$ consists of isomorphism classes of pairs (E, C_N) of a "generalised" elliptic curve E and a cyclic subgroup C_N of order N in E. We denote by $[(E, C_N)]$ an arbitrary point of

$X_0(N)$. A point $x \in X_0(N)$ is a K-rational point for a number field K if and only if there is a representative (E, C_N) for the point x such that E and C_N are defined over K. For $X_1(N)$, we have a similar property: $X_1(N)$ consists of isomorphism classes of a generalised elliptic curve E together with a point P of exact order N. Thus, we have a canoncal map $X_1(N) \longrightarrow X_0(N)$ defined by $[(E, P)] \longmapsto [(E, \langle P \rangle)]$. This map is called the *Shimura cover*.

Let $J_0(N)$ be the Jacobian of the curve $X_0(N)$. General definition of Jacobians of a curve is well discussed in the appendix *Curves and their Jacobians* to [Mum]. We ignore entirely about the geometric structure and properties of $J_0(N)$, but as an abstract group, we note that $J_0(N) = \mathrm{Pic}^0(X_0(N))$. Likewise, we have $J_1(N) = \mathrm{Pic}^0(X_1(N))$. In particular, the Shimura cover yields the canonical map on Jacobians via Picard functoriality: $J_0(N) \longrightarrow J_1(N)$. The kernel $\Sigma(N)$ of this map is called the *Shimura subgroup of* $J_0(N)$.

Now we define *Hecke operators on* $J_0(N)$. Fix a prime p with $p \nmid N$, and consider the following correspondence:

$$\begin{array}{ccc} & X_0(pN) & \\ {\scriptstyle\alpha}\swarrow & & \searrow{\scriptstyle\beta} \\ X_0(N) & & X_0(N), \end{array}$$

where the maps α and β are defined as follows. First, we write an arbitrary element of $X_0(pN)$ as a triple $[(E, C_p \times C_N)]$, as we saw before. Then,

$$\begin{aligned} \alpha &: [(E, C_p \times C_N)] \longmapsto [(E, C_N)], \\ \beta &: [(E, C_p \times C_N)] \longmapsto [(E/C_p, (C_p \times C_N)/C_p)]. \end{aligned}$$

This *Hecke correspondence* defines via divisor group $\mathrm{Div}(X_0(N))$ the Hecke operator

$$T_p : J_0(N) \longrightarrow J_0(N),$$

i.e., if we write α^* (resp. β_*) as homomorphisms $J_0(N) \longrightarrow J_0(pN)$ (resp. $J_0(pN) \longrightarrow J_0(N)$) obtained from α (resp. β) by Picard functoriality (resp. Albanese functoriality), then $T_p = \beta_* \circ \alpha^*$. Similarly, for primes $q \mid N$, we can define Hecke operators $T_q : J_0(N) \longrightarrow J_0(N)$. When we need to distinguish primes dividing N from ones

not dividing N, we use the notation $U_q = T_q$ for $q \mid N$. Also, for convenience, for any integer $n \in \mathbf{Z}_{\geq 1}$, we let T_n be the operators satisfying the following formal Dirichlet series:

$$\sum_{n\geq 1} T_n n^{-s} = \prod_{p\nmid N} \left(1 - T_p p^{-s} + p^{1-2s}\right)^{-1} \prod_{q\mid N} \left(1 - T_q q^{-s}\right)^{-1}. \tag{2.6}$$

This makes Hecke operators multiplicative, i.e., $T_m T_n = T_{mn}$ whenever $\gcd(m, n) = 1$. Let $\mathbf{T}$ be the $\mathbf{Z}$-algebra generated by all Hecke operators T_n for $n \geq 1$. It is a subalgebra called *Hecke algebra* of $\mathrm{End}_{\mathbf{C}}(J_0(N))$, and is commutative. Moreover, let $\mathbf{T}^0$ be the subalgebra of $\mathbf{T}$ generated by only those T_n with $\gcd(n, N) = 1$. For the structure of the Hecke algebras, we have the following theorem.

Theorem 2.23. *The Hecke algebras* $\mathbf{T}$ *and* $\mathbf{T}^0$ *are finitely generated as* $\mathbf{Z}$*-modules. The rank of* $\mathbf{T}$ *is equal to the genus of* $X_0(N)$*, which is also equal to* $\dim J_0(N)$*.*

Proof. Propositions II.2 through II.4 in [Dar04]. □

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbf{Z})$, i.e., $\Gamma \leq \mathrm{SL}_2(\mathbf{Z})$ contains a principal congruence subgroup $\Gamma(N)$, which consists of matrices in $\mathrm{SL}_2(\mathbf{Z})$ congruent to $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ modulo N. The largest such integer N is called the *level of the congruence subgroup* Γ. Note that Γ is of finite index in $\mathrm{SL}_2(\mathbf{Z})$. For example, the subgroups $\Gamma_0(N)$ and $\Gamma_1(N)$ are congruence subgroups of level N. For convenience, we assume the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is contained in Γ. Note that the above two groups $\Gamma_0(N)$ and $\Gamma_1(N)$ satisfy this assumption. By a *modular form of weight* k *on* Γ we mean a holomorphic function $f : \mathfrak{H} \longrightarrow \mathbf{C}$ satisfying

(i) $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, and

(ii) for any $\gamma \in \mathrm{SL}_2(\mathbf{Z})$, the function $f|\gamma(\tau) := (c\tau + d)^{-k} f(\gamma\tau)$ can be written as

$$\sum_{n\geq 0} a_n^{\gamma} q^n, \tag{2.7}$$

where $q = e^{2\pi i\tau}$.

The expression (2.7) is called the *q-expansion at the cusp* $\gamma^{-1}\infty$. We also say a modular form f is a *cusp form* if $a_n^\gamma = 0$ for all $\gamma \in \mathrm{SL}_2(\mathbf{Z})$. By $S_k(\Gamma)$ we denote the $\mathbf{C}$-vector space of cusp forms of weight k on Γ.

The Hecke operators also act linearly on the space of cusp forms $S_2(N) := S_2(\Gamma_0(N))$. The Hecke action on the q-expansion at the cusp ∞ of a cusp form $f = \sum_{n\geq 1} a_n q^n \in S_2(N)$ is given as follows:

$$T_p f = \begin{cases} \sum_{p|n} a_n q^{n/p} + p \sum a_n q^{pn} & \text{if} p \nmid N, \\ \sum_{p|n} a_n q^{n/p} & \text{if} p \mid N. \end{cases}$$

The $\mathbf{C}$-vector space $S_2(N)$ is equipped with a non-degenerate Hermitian inner product

$$\langle f, g \rangle = \int_{\Gamma_0(N)\backslash \mathfrak{H}^*} f(\tau)\overline{g(\tau)} dx dy,$$

called the *Petersson inner product*. The Hecke operators $T_p \in \mathbf{T}^0$ acts as self-adjoint operators in $S_2(N)$ with respect to the Petersson inner product. We say a modular form f is an *eigenform* if it is a simultaneous eigenvector for all the Hecke operators in $\mathbf{T}$, i.e., there is a ring homomorphism $\lambda : \mathbf{T} \longrightarrow \mathbf{C}$ such that $Tf = \lambda(T)f$ for all $T \in \mathbf{T}$. By a direct calculation, if f is an eigenform then the coefficients of the q-expansion $a_n(f)$ at the cusp ∞ is given by the formula

$$a_n(f) = a_1(f)\lambda(T_n).$$

We call an eigenform having $a_1(f) = 1$ a *normalised eigenform*. By the relation of the coeffients given above, if a ring homomorphism $\lambda : \mathbf{T} \longrightarrow \mathbf{C}$ is given, then the corresponding *eigenspace*

$$S_\lambda = \{f \in S_2(N) : Tf = \lambda(T)f \text{ for all } T \in \mathbf{T}\}$$

is one dimensional, and the eigenform $f \in S_\lambda$ forms a basis. This is very important, and in literatures, the result is called *multiplicity one theorem*.

However in general, the space $S_2(N)$ is not decomposed into a direct sum of eigenspaces S_λ. This is due to the fact that the operators in $\mathbf{T}$ do not act semi-simply on $S_2(N)$. We can remedy this by adopting another subspace of $S_2(N)$ on which

$\mathbf{T}$ acts semi-simply. This subspace is called the *space of newforms* and is denoted by $S_2^{\mathrm{new}}(N)$. More precisely, we let $S_2^{\mathrm{old}}(N)$ be the subspace of $S_2(N)$ consisting of linear combinations of those forms $f \in S_2(N)$ such that there exists a cusp form $g \in S_2(N/d)$ for some divisor $d \neq 1$ of N, and $f(\tau) = g(d'\tau)$ for some $d' \mid d$. Such forms as f are called *oldforms*, and the space of newforms $S_2^{\mathrm{new}}(N)$ is the orthogonal complement of $S_2^{\mathrm{old}}(N)$ with respect to the Petersson inner product.

Theorem 2.24 (Atkin–Lehner)**.** *The space of newforms $S_2^{\mathrm{new}}(N)$ is decomposed as*

$$S_2^{\mathrm{new}}(N) = \bigoplus_{\lambda} \mathbf{C} f_\lambda,$$

where λ runs over all ring homomorphisms $\mathbf{T} \longrightarrow \mathbf{C}$, and $f_\lambda(\tau) = \sum_{n\geq 1} \lambda(T_n) q^n$ are normalised eigenforms.

Proof. See [AtLe]. □

For simplicity, we call such f_λ just a *newform of level N*. For a newform f of level N, we define the L-series of f as follows.

$$L(f,s) = \sum_{n=1}^{\infty} a_n(f) n^{-s}. \tag{2.8}$$

Initially, we can show that $L(f,s)$ is defined on the half plane $\mathrm{Re}\, s > 3/2$.

Theorem 2.25. *The L-series of a newform f of level N satisfies the following properties.*

(i) $L(f,s)$ admits the Euler product

$$L(f,s) = \prod_{p \nmid N} \left(1 - a_p(f) p^{-s} + p^{1-2s}\right)^{-1} \prod_{q \mid N} \left(1 - a_q(f) q^{-s}\right)^{-1}.$$

Noteworthily enough, we now see the reason Hecke operators T_n for non-prime n are defined in such a way as in Equation (2.6)*.*

(ii) Let $\Lambda(f,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(f,s)$ be the completed L-series. Then,

$$\Lambda(f,s) = N^{s/2} \int_0^{\infty} f(iy) y^{s-1} dy.$$

Thus $\Lambda(f,s)$ (and hence $L(f,s)$) can be analytically continued to be an entire function on $\mathbf{C}$.

(iii) We have the functional equation

$$\Lambda(f, s) = -\Lambda(W_N(f), 2 - s),$$

where W_N is the Atkin–Lehner involution.

Proof. (i) directly follows by the definition of Hecke operators T_n and Fourier coefficients $a_n(f)$. For (ii) and (iii), see §5 in [DiIm]. □

Note the similarity of Hasse–Weil L-functions for elliptic curves and the above L-functions for newforms. It is not a coincidence, and there are some deep relations showing close interconnection between elliptic curves and newforms. Even more than that, we dare to claim that they are essentially the same objects in view of arithmetic. The following theorem provides one direction of this interdependence.

Theorem 2.26 (Eichler–Shimura)**.** *Let f be a normalised eigenform whose Fourier coefficeints $a_n(f)$ are in $\mathbf{Z}$. Then there exists an elliptic curve E_f defined over $\mathbf{Q}$ such that*

$$L(f, s) = L(E_f/\mathbf{Q}, s).$$

Proof. Here we are content ourselves with seeing the construction of E_f from f. For the remainder of the proof, the reader may consult §I.7 in [DDT]. Recall that we take $X_0(N)$ to be an algebraic curve defined over $\mathbf{Q}$, whose complex points form a compact Riemann surface $X_0(N)(\mathbf{C}) = \Gamma_0(N)\backslash\mathfrak{H}^*$. Also recall that $J_0(N)$ is the Jacobian variety of $X_0(N)$ defined over $\mathbf{Q}$. Let I_f be the kernel of the ring homomorphism $\lambda : \mathbf{T} \longrightarrow \mathbf{C}$ attached to f. Now we define $E_f := J_0(N)/I_f J_0(N)$. The rest of the proof is to compare $a_p(E_f) := 1 + p - \#\widetilde{E_f}(\mathbf{F}_p)$ when E_f has good reduction at p with Fourier coefficients $a_p(f)$. □

Corollary 2.27 (Carayol)**.** *The level N of the newform f is equal to the conductor of E_f.*

Proof. See [Car]. □

Now we develop converse statements.

Definition. An elliptic curve $E/\mathbf{Q}$ of conductor N is *modular* if there is a newform $f = f_E \in S_2^{\mathrm{new}}(N)$ such that $L(E/\mathbf{Q}, s) = L(f, s)$.

Corollary 2.28. *Suppose that $E/\mathbf{Q}$ is a modular elliptic curve. Then the Hasse–Weil conjecture 2.22 is true for E.*

Proof. This is immediate from Theorem 2.25. □

Suppose that $E/\mathbf{Q}$ is an elliptic curve. Note that Faltings' theorem ([Fal]) says that two elliptic curves are isogenous if and only if they have the same L-function. So, if $E/\mathbf{Q}$ is modular, then by Eichler–Shimura construction 2.26 we have an isogeny $E_f = J_0(N)/I_f J_0(N) \longrightarrow E$ for some newform f of level N. Composing with the canonical embedding

$$X_0(N) \longrightarrow J_0(N), \qquad x \longmapsto [(x) - (\infty)],$$

we have a morphism $X_0(N) \longrightarrow E$. This is called the *modular parametrisation of E*. In fact, the existence of such a modular parametrisation is equivalent to E being modular.

The following is a groundbreaking theorem. It is proved for semistable elliptic curves by Wiles [Wil] plus some corrections with Taylor [TaWi], and unconditionally by Breuil, Conrad, Diamond and Taylor ([BCDT]).

Theorem 2.29 (Modularity theorem)**.** *Every elliptic curve E over $\mathbf{Q}$ is modular.*

We close this section with defining one more important invariant of modular elliptic curve. Let $\pi : X_0(N) \longrightarrow E$ be a modular parametrisation over $\mathbf{Q}$, and let ω be the *Néron differential of E*, i.e., it is the minimal differential of a minimal model of E. Manin ([Man]) showed that $\pi^*\omega = M \cdot 2\pi i f(\tau) d\tau$, for a constant $M \in \mathbf{Q}^\times$.

Conjecture 2.30 (Manin)**.** $M = 1$ for $X_0(N)$-optimal curves, which are curves of the form E_f.[5]

Definition. Let $\pi : X_0(N) \longrightarrow E$ be a modular parametrisation. The constant M such that $\pi^*\omega = M \cdot 2\pi i f(\tau) d\tau$ is called the *Manin constant of the modular parametrisation*.

For current status of the Manin's conjecture, see [ARS].

[5]For the precise definition of and some discussions about optimal curves, see §3.1.

2.9 Birch and Swinnerton-Dyer conjecture

Let K be a number field, and let E be an elliptic curve defined over K. The essence of the arithmetic of E/K is to determine the Mordell–Weil group $E(K)$. By Theorem 2.15, the group is finitely generated, and so we can divide the group into free and torsion parts. It is generally much harder to determine the free part of the Mordell–Weil group. The following conjecture is essentially a bridge, between the arithmetic of the free part of $E(K)$ and the analysis of the L-function $L(E/K, s)$.

Conjecture 2.31 (Birch and Swinnerton-Dyer)**.** Let E be an elliptic curve defined over a number field K. We assume the Hasse–Weil L-series of E/K has meromorphic continuation to all of $\mathbf{C}$ (cf. Conjecture 2.22).

(i) The rank r of the curve E is equal to the order of zero of the Hasse–Weil L-function of E over K at $s = 1$, i.e., $r = \mathrm{ord}_{s=1} L(E/K, s)$.

(ii) The leading coefficient of $L(E/K, s)$ at $s = 1$ is

$$\mathrm{BSD}(E/K) := \frac{\#Ш(E/K) \cdot \mathrm{Reg}(E/K) \cdot P(E/K)}{(\#E(K)_{\mathrm{tors}})^2}. \tag{2.9}$$

One of curious things which can be revealed at a glance is that Conjecture 2.31 was formulated upon another conjectures: in order to evaluate the L-function at $s = 1$, we need the analytic continuity property of the L-function, and in the formula (2.9), one need the finiteness of the Tate–Shafarevich group $Ш(E/K)$. In [Tat74], Tate wrote on the BSD conjecture:

> "This remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined to the order of the group Ш which is not known to be finite!"[6]

In fact, the latter is a conjecture of Tate and Shafarevich.

Conjecture 2.32 (Tate–Shafarevich)**.** For any elliptic curves E over K, the Tate–Shafarevich group $Ш(E/K)$ is finite.

[6] [Tat74], p. 198.

The other quantities in the formula (2.9) are already defined in this dissertation. Recall $\mathrm{Reg}(E/K)$ is the elliptic regulator for E/K defined in 2.6. One thing we define now is the invariant $P(E/K)$.

Definition. The *period of* E/K is

$$P(E/K) = \prod_{\mathfrak{p} \nmid \infty} \left(F_{\mathfrak{p}}(q_{\mathfrak{p}}^{-1})^{-1} \cdot \int_{E(K_{\mathfrak{p}})} |\omega_{\mathfrak{p}}| \right) \cdot \prod_{\mathfrak{p} \mid \infty} \int_{E(K_{\mathfrak{p}})} |\omega_{\mathfrak{p}}|, \tag{2.10}$$

where $F_{\mathfrak{p}}(T)$ is the local polynomial (cf. §2.7):

$$F_{\mathfrak{p}}(T) = \begin{cases} 1 - a_{\mathfrak{p}}T + q_{\mathfrak{p}}T^2 & \text{if } E/K \text{ has good reduction at } \mathfrak{p}, \\ 1 - T & \text{if } E/K \text{ has split multiplicative reduction at } \mathfrak{p}, \\ 1 + T & \text{if } E/K \text{ has non-split multiplicative reduction at } \mathfrak{p}, \\ 1 & \text{if } E/K \text{ has additive reduction at } \mathfrak{p}, \end{cases}$$

and ω is an invariant differential for E/K.

This definition does not depend on the choice of the invariant differential. By the change of variables formula 2.1, two distinct invariant differentials ω and ω' for E/K are related as $\omega' = u\omega$ for some $u \in K^\times$. But then changing $\omega \longrightarrow \omega'$ only modifies $P(E/K)$ by the factor of $\prod_{\mathfrak{p}} |u|_{\mathfrak{p}} = 1$, by the product formula (cf. Proposition III.1.3 in [Neu99]).

When E/K has a Néron differential, which is possible when E/K has a global minimal model, then the $P(E/K)$ can be expressed in a simpler way. By computing the integral for finite primes in the formula 2.10 (cf. [Gro11], Lecture 2, Lemma 19), we have

$$P(E/K) = \prod_{\mathfrak{p} \text{ bad}} [E(K_{\mathfrak{p}}) : E^0(K_{\mathfrak{p}})] \cdot \prod_{\mathfrak{p} \mid \infty} \int_{E(K_{\mathfrak{p}})} |\omega_{\mathfrak{p}}| \cdot |\operatorname{disc}(K)|^{-1/2},$$

where $\operatorname{disc}(K)$ is the absolute discriminant of the field $K/\mathbf{Q}$. Note the appearance of the Tamagawa numbers $C_{\mathfrak{p}} = [E(K_{\mathfrak{p}}) : E^0(K_{\mathfrak{p}})]$. Some authors avoid using this complicated formula for $P(E/K)$ and simply express the BSD formula 2.9 as follows, at least when E/K has a Néron differential.

$$\mathrm{BSD}(E/K) = \frac{\#Ш(E/K) \cdot \mathrm{Reg}(E/K) \cdot C(E/K) \cdot \Omega(E/K)}{(\#E(K)_{\mathrm{tors}})^2 \cdot \sqrt{|\operatorname{disc}(K)|}}, \tag{2.11}$$

where

$$C(E/K) = \prod_{\mathfrak{p} \text{ bad}} [E(K_\mathfrak{p}) : E^0(K_\mathfrak{p})]$$

$$\Omega(E/K) = \prod_{\mathfrak{p}|\infty} \int_{E(K_\mathfrak{p})} |\omega_\mathfrak{p}|.$$

Chapter 3

Differing isogenies of optimal curves

> "I don't know where I'm going from here, but I promise it won't be boring."
>
> David Bowie

3.1 Optimal curves and étale isogenies

Let $E/\mathbf{Q}$ be an elliptic curve. By Wiles' theorem 2.29, we know the existence of a newform f such that

$$L(E/\mathbf{Q}, s) = L(f, s) = L(E_f/\mathbf{Q}, s).$$

The curve E_f is isogenous to E, and it is called the $X_0(N)$*-optimal curve of the isogeny class* $\mathcal{C}$ *of* E (or, in a slightly older terminology, *strong Weil curve (for* $X_0(N)$*)*).

In [Ste], Stevens suggested that modular parametrisation for E of the curve $X_1(N)$ is better and has simple properties than of $X_0(N)$. We can also define optimal curves for $X_1(N)$ by a similar fashion. In this section, we review these modular

parametrisations and some conjectural intrinsic characterisation for $X_1(N)$-optimal curves.

We define $X_i(N)$-optimal curves for $i = 0, 1$ more precisely.

Proposition 3.1. *Let C be an isogeny class of modular elliptic curves with conductor N. For $i = 0, 1$, there is a unique curve E_i and a parametrisation $\pi_i : X_i(N) \longrightarrow E_i$ satisfying the following equivalent properties.*

(i) For any $E \in C$ and for any parametrisation $\pi : X_i(N) \longrightarrow E$, there exists an isogeny $\phi : E_i \longrightarrow E$ making the following diagram commutative:

$$\begin{array}{ccc} X_i(N) & & \\ {\scriptstyle \pi_i}\downarrow & \searrow^{\pi} & \\ E_i & \xrightarrow{\phi} & E. \end{array}$$

(ii) The induced map on homology groups $H_1(X_i(N)(\mathbf{C}), \mathbf{Z}) \longrightarrow H_1(E_i(\mathbf{C}), \mathbf{Z})$ is surjective.

(iii) The induced map $E_i \cong \mathrm{Pic}^0(E_i) \longrightarrow \mathrm{Pic}^0(X_i(N)) =: J_i(N)$ is injective.

Proof. [Maz72a], Lemme 3. □

Definition. The unique curve E_i in the above proposition is called the *$X_i(N)$-optimal curve in C*.

One of the main reason Stevens voted for $X_1(N)$-optimal curves is, at least conjecturally, $X_1(N)$-optimal curves are classified intrinsically, without refering to modular parametrisations, in terms of étale isogenies. In order to look at Stevens' arguments, we need to settle the definition and some properties of étale isogenies.

Definition. An isogeny $\phi : E \longrightarrow E'$ of elliptic curves over $\mathbf{Q}$ is called *étale* if its extension to Néron models is an étale morphism.

An *étale morphism* is defined by a smooth morphism of relative dimension 0 and is an algebro-geometric analogue of local isomorphisms in topology. For detailed illustrations of étale morphisms, see [BLR] §III.2, [Mil80] chapter I, or [Fu] chapter II.

Proposition 3.2. *Let $\phi : E \longrightarrow E'$ be an isogeny over $\mathbf{Q}$, and let $\phi_{\mathbf{Z}} : E_{\mathbf{Z}} \longrightarrow E'_{\mathbf{Z}}$ be its extension to Néron models. Let ω (resp. ω') be the Néron differential for E (resp. for E').*

(i) The isogeny ϕ is étale if and only if ϕ induces an isomorphism on Néron differentials

$$\phi^* : H^0(E'_{\mathbf{Z}}, \Omega^1_{E'_{\mathbf{Z}}/\mathbf{Z}}) \xrightarrow{\sim} H^0(E_{\mathbf{Z}}, \Omega^1_{E_{\mathbf{Z}}/\mathbf{Z}})$$

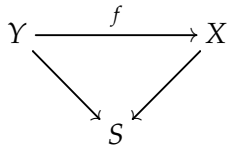
(ii) We have $\phi^*\omega' = n_\phi \omega$, for some nonzero $n_\phi \in \mathbf{Z}$. Then the isogeny ϕ is étale if and only if $n_\phi = \pm 1$.

(iii) If ϕ is any isogeny of prime degree, then precisely one of ϕ or its dual ϕ' is étale.

(iv) The composition of two étale isogenies is also étale.

(v) Suppose that ϕ is a cyclic isogeny[1] of odd prime degree ℓ. Then it is étale if and only if its kernel is isomorphic to $\mathbf{Z}/\ell\mathbf{Z}$ as a $G_{\mathbf{Q}}$-module.

Proof. (i), (ii) For a morphism $f : Y \longrightarrow X$ of schemes, by $\Omega^1_{Y/X}$ we denote the sheaf of relative Kähler differentials with respect to the morphism f. Suppose we have the following diagram of smooth morphisms



of schemes. Then we have the exact sequence

$$0 \longrightarrow f^*\Omega^1_{X/S} \longrightarrow \Omega^1_{Y/S} \longrightarrow \Omega^1_{Y/X} \longrightarrow 0$$

(Proposition II.5.4 in [Fu]). If f is étale, then it is of relative dimension 0, and thus $\Omega^1_{Y/X} = 0$. In particular when $Y = E_{\mathbf{Z}}$, $X = E'_{\mathbf{Z}}$ and $S = \operatorname{Spec} \mathbf{Z}$, we have $H^0(E_{\mathbf{Z}}, \Omega^1_{E_{\mathbf{Z}}/\mathbf{Z}}) = \mathbf{Z}\omega$ and $H^0(E'_{\mathbf{Z}}, \Omega^1_{E'_{\mathbf{Z}}/\mathbf{Z}}) = \mathbf{Z}\omega'$, it follows that $n_\phi = \pm 1$. The converse is similar.

(iii) Since $\phi' \circ \phi = [\ell]$ for some prime ℓ, and $[\ell]^*\omega = \ell\omega$ (Corollary III.5.3 in [Sil09]), we have either $n_\phi = \pm 1$ or $n_{\phi'} = \pm 1$.

(iv) This follows from the same property of étale morphisms.

(v) This follows from the classification of étale group schemes. □

[1] An isogeny is *cyclic* if its kernel is a cyclic group.

We can choose another representative among the curves in the isogeny class C other than optimal curves. Étale isogenies play a crucial role to pick such a representative.

Theorem 3.3 (Stevens)**.** *In any isogeny class C of elliptic curves over $\mathbf{Q}$, there is a unique curve $E_{\min}$ satisfying the following equivalent condition.*

(i) For every $E \in C$, there is an étale isogeny $\phi : E_{\min} \longrightarrow E$.

(ii) For every $E \in C$, we have $L(E_{\min}) \subseteq L(E)$, where $L(E)$ is the lattice of Néron period *defined by*

$$L(E) := \operatorname{im}\left(H_1(E(\mathbf{C}), \mathbf{Z}) \xrightarrow{\int \omega} \mathbf{C}\right),$$

where ω is the Néron differential on E.

(iii) For every $E \in C$, we have $H(E_{\min}) \leq H(E)$, where $H(E)$ is the Faltings–Parshin height of E *defined by*

$$H(E) = \frac{1}{\operatorname{covolume}(L(E))} = \left(\frac{1}{2\pi i}\int_{E(\mathbf{C})} \omega \wedge \overline{\omega}\right)^{-1/2},$$

where ω is the Néron differential on E.

Proof. [Ste], Theorem 2.3. □

It turns out that the étale minimal curve $E_{\min}$ is closely related to $X_1(N)$-optimal curve E_1. In fact, Stevens conjectured that they are actually the same.

Conjecture 3.4 (Stevens)**.** In every isogeny class C of curves of conductor N over $\mathbf{Q}$, the $X_1(N)$-optimal curve E_1 is equal to $E_{\min}$.

Later, Vatsal showed the conjecture is true up to an isogeny of degree a power of 2, when the conductor N is square-free.

Theorem 3.5 (Vatsal)**.** *Suppose that the isogeny class C consists of semi-stable curves. The étale isogeny $\phi : E_{\min} \longrightarrow E_1$ has degree a power of two.*

Proof. [Vat], Theorem 1.10. □

3.2 Differing isogenies: Stein–Watkins conjecture

It seems that for most isogeny classes C, the optimal curves E_0 and E_1 are the same. However, there are also several examples of isogeny classes with non-isomorphic optimal curves. For example, $E_0 = X_0(11)$ and $E_1 = X_1(11)$ differ by a 5-isogeny. Based on numerical computations, Stein and Watkins [StWa02] made a precise conjecture which classifies isogeny classes with non-isomorphic optimal curves. According to [StWa02], in any isogeny class C, the optimal curves E_0 and E_1 are only isogenous by an isogeny of degree 1 (when $E_0 = E_1$), 2^n for some $n \geq 1$, 3, or 5.

Conjecture 3.6 (Stein–Watkins)**.**

(i) There are three major cases when the optimal curves differ by a 2-isogeny.

   (a) Neumann–Setzer curves; parametrised by $c_4 = p - 16$ and $c_6 = u(p + 8)$, with the discriminant $p = u^2 + 64$ being a prime and u being taken to be congruent to 3 modulo 4.

   (b) Curves parametrised by $c_4 = 16P - 16$ and $c_6 = 4v(16P + 8)$ with $v \equiv 3 \pmod 4$ and P being prime. The conductor is $4P$.

   (c) Curves parametrised by $c_4 = PQ + 16$ and $c_6 = (P + 8)(PQ - 8)$ with P and $Q = P + 16$ both being primes.

(ii) E_0 and E_1 differ by a 3-isogeny if and only if there is an elliptic curve $E \in C$ given by

$$c_4 = (n + 3)(n^3 + 9n^2 + 27n + 3)$$

and

$$c_6 = -(n^6 + 18n^5 + 135n^4 + 504n^3 + 891n^2 + 486n - 27),$$

with discriminant being $n(n^2 + 9n + 27)$, where $n^2 + 9n + 27$ is a prime power and n has no prime factors congruent to 1 modulo 6.

(iii) E_0 and E_1 differ by a 5-isogeny if and only if the isogeny class is '11a'.

Many mathematicians including Stein and Watkins themselves have been interested in Neumann–Setzer curves. Systematic investigations are begun by Neumann

([Neum]) and Setzer ([Set]). They proved that for each prime $p = u^2 + 64$, there are actually two curves in the isogeny class (cf. Theorem 2 in [Set]), namely

$$\text{SN A}(p) : y^2 + xy = x^3 + \frac{u-1}{4}x^2 + 4x + u,$$

and

$$\text{SN B}(p) : y^2 + xy = x^3 + \frac{u-1}{4}x^2 - x$$

(notations followed from [MeOe]; they actually take the convention $u \equiv 1 \pmod 4$). In [MeOe], Mestre and Oesterlé showed SN A(p) is the $X_0(p)$-optimal curve in the isogeny class. Much later, in [StWa04], Stein and Watkins proved that the curve SN B(p) has smaller Faltings–Parshin height than SN A(p), i.e., SN B(p) is the étale minimal curve, and in fact SN B(p) is $X_1(p)$-optimal.

In [ByYh13], Byeon and Yhee proved that the Stein–Watkins conjecture for the case of 3-isogeny (3.6 (ii)) needs to be modified slightly, and the modified conjecture is true.

Theorem 3.7 (Byeon–Yhee; Theorem 1.1 in [ByYh13])**.** *Let $\mathcal{C}$ be an isogeny class of elliptic curves over $\mathbf{Q}$ of conductor N. Consider the following statements:*

(i) there is an elliptic curve $E \in \mathcal{C}$ given by $y^2 + (n+3)xy + y = x^3$ where n is an integer such that $n^2 + 9n + 27$ is a prime power and n has no prime factors congruent to 1 modulo 6,

(ii) optimal curves E_0 and E_1 in $\mathcal{C}$ differ by a 3-isogeny.

Then (i) implies (ii), and if N is square-free and $3 \nmid N$, then (ii) also implies (i).

Remark. The unmodified original conjecture made by Stein and Watkins for this case claimed the equivalence of (i) and (ii).

The goal of this chapter is to prove the following analogue for the 5-isogeny case.

Theorem 3.8 (Main theorem for Chapter 3)**.** *For $i = 0, 1$, let E_i be the $X_i(N)$-optimal curve of an isogeny class $\mathcal{C}$ of elliptic curves defined over $\mathbf{Q}$ of conductor N. Suppose that N is square-free and $5 \nmid N$. Then E_0 and E_1 differ by a 5-isogeny if and only if $E_0 = X_0(11)$ and $E_1 = X_1(11)$.*

Remark. We also have altered the original conjecture as in Byeon–Yhee Theorem 3.7 to insist N is square-free and not divisible by 5. Otherwise the conjecture is not true. For example, assuming Stevens's conjecture 3.4, consider the isogeny class '33825be' in Cremona's database of elliptic curves ([Cre]). In this case, the curves '33825be1' and '33825be3' are $X_0(33825)$- and $X_1(33825)$-optimal curves, respectively.

3.3 Falsity of Hadano's conjecture

Let E be an elliptic curve over $\mathbf{Q}$ of conductor N having a rational torsion point of order n and p be a prime dividing n. In [Had], Hadano considered whether the p-isogenous curve E' to E possesses a rational torsion point of order n again. In this section, we consider the case when $n = p = 5$. For this case, Hadano's work can be restated as following.

When a rational elliptic curve E has a rational 5-torsion point, we can take a Weierstrass equation for E as follows:

$$y^2 + (v-u)xy - uv^2y = x^3 - uvx^2 \tag{3.1}$$

where $u, v \in \mathbf{Z}$ with $\gcd(u,v) = 1$ and $u > 0$. Note that the discriminant Δ of E is given by

$$\Delta = u^5v^5(u^2 - 11uv - v^2)$$

and the rational torsion subgroup is

$$T = \left\{\infty, (0,0), (uv, u^2v), (uv, 0), (0, uv^2)\right\}.$$

Lemma 3.9. *The Weierstrass equation of the form* (3.1) *with* $u, v \in \mathbf{Z}$, $\gcd(u,v) = 1$, *and* $u > 0$ *is minimal.*

Proof. We only need to check the minimality of the equation (3.1) for primes dividing $\Delta = u^5v^5(u^2 - 11uv - v^2)$. For primes p dividing uv, we can obtain minimality by simply looking at the order of the constant c_4: indeed, $\mathrm{ord}_p\, c_4 = 0$. Suppose that a prime p divides $(u^2 - 11uv - v^2)$, and assume $\mathrm{ord}_p\, \Delta = \mathrm{ord}_p(u^2 - 11uv - v^2) \geq 12$.

Note that in this case p can divide neither u nor v, because $\gcd(u, v) = 1$. Since $c_4 = u^4 - 12u^3v + 14u^2v^2 + 12uv^3 + v^4$, by dividing c_4 by $u^2 - 11uv - v^2$, we have

$$c_4 = (u^2 - 11uv - v^2)(-4u^2 - uv - v^2) + 5u^3(u - 11v).$$

If $p \mid c_4$, then we must have $p = 5$ or $p \mid (u - 11v)$ (or both). If $p \mid (u - 11v)$, then since $u^2 - 11uv - v^2 = (u - 11v)u - v^2$, we must have $p \mid v$, a contradiction. Thus, in any remaining cases, we have $\operatorname{ord}_p c_4 \leq 1$, and hence the equation is minimal at p. □

Let E' be an elliptic curve defined by $E' = E/T$. We use Vélu's formula to find a Weierstrass equation for E' (cf. [MMR]). Applying to Equation (3.1), we get a Weierstrass equation for E' of the following form:

$$\begin{aligned} y^2 + (v - u)xy - uv^2y & \\ &= x^3 - uvx^2 + (5uv^3 - 10u^2v^2 - 5u^3v)x \\ &\qquad + (uv^5 - 15u^2v^4 + 5u^3v^3 - 10u^4v^2 - u^5v) \end{aligned} \tag{3.2}$$

with discriminant $\Delta' = uv(u^2 - 11uv - v^2)^5$.

Lemma 3.10. *The Weierstrass equation* (3.2) *with* $u, v \in \mathbf{Z}$, $\gcd(u, v) = 1$, *and* $u > 0$ *is minimal, possibly outside of the prime* $p = 5$.

Proof. We only need to consider for primes p dividing $\Delta' = uv(u^2 - 11uv - v^2)^5$. Note that the c_4-invariant c_4' of E' is given as follows:

$$\begin{aligned} c_4' &= u^4 + 228u^3v + 494u^2v^2 - 228uv^3 + v^4 \\ &= (u^2 - 11uv - v^2)(-3124u^2 + 239uv - v^2) + 5^5u^3(u - 11v). \end{aligned}$$

If p divides uv, then because $\gcd(u, v) = 1$, the invariant c_4' has order 0 at p and thus the equation is minimal at p. Suppose that p divides $u^2 - 11uv - v^2$. In order to show minimality, assume to the contrary that $\operatorname{ord}_p(u^2 - 11uv - v^2) \geq 3$ and $\operatorname{ord}_p c_4' \geq 4$. As $p \nmid u$ and $p \nmid v$, and since $u^2 - 11uv - v^2 = (u - 11v)u - v^2$, we must have $p = 5$ and $p \nmid (u - 11v)$. □

Remark. Suppose that the equation (3.2) is not minimal at $p = 5$. This is equivalent to say that $5 \nmid uv$, $\operatorname{ord}_5 \Delta' \geq 12$ and $\operatorname{ord}_5 c_4' \geq 4$. Using the formula for c_4' given in the proof above, we can see that $\operatorname{ord}_5 c_4'$ must be exactly 5. So the minimal discriminant of E' is exactly $\Delta'/5^{12}$ in this case.

In order that E' has a rational point of order 5 again, the equation must be transformed into the form

$$y^2 + (V - U)xy - UV^2y = x^3 - UVx^2 \tag{3.3}$$

for some $U, V \in \mathbf{Z}$ with $(U, V) = 1$ and $U > 0$. Since the equations (3.2) and (3.3) must define the same curve, we can compare their discriminants and c_4-invariants. Since the equation (3.3) is minimal (cf. Lemma 3.9), we have

$$uv(u^2 - 11uv - v^2)^5 = 5^{12k}U^5V^5(U^2 - 11UV - V^2) \tag{3.4}$$

and

$$v^4 - 228uv^3 + 494u^2v^2 + 228u^3v + u^4 = 5^{4k}(V^4 + 12UV^3 + 14U^2V^2 - 12U^3V + U^4), \tag{3.5}$$

for some $k \in \{0, 1\}$ chosen accordingly whether the equation (3.2) is minimal or not.

Let $r = \dfrac{u^2 - 11uv - v^2}{UV} \in \mathbf{Q}$. Then we have

$$\begin{aligned} UVr &= u^2 - 11uv - v^2, \\ uvr^5 &= 5^{12k}(U^2 - 11UV - V^2). \end{aligned} \tag{3.6}$$

Set $s = v/u \in \mathbf{Q}$. If we write $f(x, y) = x^2 - 11xy - y^2$, then the right hand side of the equation (3.5) can be written as $5^{4k}(f(U, V)^2 + 10UVf(U, V) + 5U^2V^2)$. We divide both sides of (3.5) by u^4 and considering the formulae (3.6) to obtain

$$\begin{aligned} & s^4 - 228s^3 + 494s^2 + 228s + 1 \\ =& \frac{5^{4k}\left(f(U, V)^2 + 10UVf(U, V) + 5U^2V^2\right)}{u^4} \\ =& \frac{r^2 5^{24k}\left(f(U, V)^2 + 10UVf(U, V) + 5U^2V^2\right)}{5^{20k}r^2u^4} \\ =& \frac{u^2v^2r^{12} + 10 \cdot 5^{12k}uvf(u, v)r^6 + 5 \cdot 5^{24k}f(u, v)^2}{5^{20k}r^2u^4} \\ =& \frac{s^2r^{12} + 2 \cdot 5^{12k+1}(s - 11s^2 - s^3)r^6 + 5^{24k+1}(1 - 22s + 119s^2 + 22s^3 + s^4)}{5^{20k}r^2}. \end{aligned} \tag{3.7}$$

By multiplying $5^{20k}r^2$ to both sides of the above equation (3.7), we get the Diophantine equation

$$5^{20k}r^2\left(s^4-228s^3+494s^2+228s+1\right)$$
$$=s^2r^{12}+2\cdot 5^{12k+1}(s-11s^2-s^3)r^6+5^{24k+1}(1-22s+119s^2+22s^3+s^4). \quad (3.8)$$

Moreover when $k=0$, we get a simpler equation

$$\left(-r^5s+5r^4s-15r^3s+25r^2s-25rs+s^2+11s-1\right)$$
$$\times\left(r^5s+5r^4s+15r^3s+25r^2s+25rs+s^2+11s-1\right)\times\left(r^2-5\right)=0.$$

Since $r\in\mathbf{Q}$, we drop the last factor to get

$$\left(s^2-1-(r^5-5r^4+15r^3-25r^2+25r-11)s\right)$$
$$\times\left(s^2-1+(r^5+5r^4+15r^3+25r^2+25r+11)s\right)=0,$$

so if we make a substitution $r+1=t$ or $r-1=t$, the above equation is equivalent to

$$s^2+(t^4+5t^2+5)st=1. \quad (3.9)$$

Unlike the case $k=0$, when $k=1$, we cannot reduce the equation (3.8) to a simpler one.

In [Had], Hadano only considered the case $k=0$, and made the following proposition. We slightly modify his proposition to cover all possible cases.

Proposition 3.11 (Hadano)**.** *If a rational elliptic curve E of conductor N has a rational point P of order 5 and $E':=E/\langle P\rangle$ has a rational point of order 5 again, then the Diophantine equation* (3.8) *has a rational solution in (r,s) (especially, the Diophantine equation* (3.9) *has a rational solution in (s,t) when $k=0$).*

We can observe that the Diophantine equation (3.9) has trivial solutions $(s,t)=(\pm 1,0)$ and these trivial solutions correspond to the elliptic curves $E=X_1(11)$ and $E'=X_0(11)$. Based on this observation and Proposition 3.11, Hadano [Had] conjectured the following.

Conjecture 3.12 (Hadano)**.** The Diophantine equation (3.9) has only trivial solutions $(s,t) = (\pm 1, 0)$. In particular, if a rational elliptic curve E has a rational point P of order 5 and $E' := E/\langle P \rangle$ has a rational point of order 5 again, then we must have $E' = X_0(11)$ and $E = X_1(11)$.

Rubin and Silverberg [RuSi] considered some families of elliptic curves with constant mod-p representations. In particular, following Klein, they defined an elliptic curve B_u over $\mathbf{Q}(u)$ as follows:

$$B_u : y^2 = x^3 - \frac{u^{20} - 228u^{15} + 494u^{10} + 228u^5 + 1}{48}x + \frac{u^{30} + 522u^{25} - 10005u^{20} - 10005u^{10} - 522u^5 + 1}{864}.$$

The curve B_u has the property that $B_u[5] \cong (\mathbf{Z}/5\mathbf{Z}) \oplus \mu_5$ as $\mathrm{Gal}(\overline{\mathbf{Q}(u)}/\mathbf{Q}(u))$-module. Using this curve, we show that the conjecture of Hadano is not true.

Theorem 3.13. *Hadano's conjecture is not true.*

Proof. By substituting a special value $u \in \mathbf{Q}$, we get an elliptic curve defined over $\mathbf{Q}$ which has its full 5-torsion subgroup isomorphic to $(\mathbf{Z}/5\mathbf{Z}) \oplus \mu_5$ as $G_{\mathbf{Q}}$-module. Hence, at least in case that B_u gives a semistable curve, we have a sequence of elliptic curves with étale isogenies

$$B_u/\mu_5 \to B_u \to B_u/(\mathbf{Z}/5\mathbf{Z}).$$

More concretely, if we substitute $u = 3$, then the curve B_u becomes the semistable curve '185163a2' in Cremona's database, and we have

$$185163\text{a}1 \to 185163\text{a}2 \to 185163\text{a}3,$$

where all arrows indicate étale isogenies. This sequence corresponds to the solution $s = -1/243$ and $t = -8/3$ of the Diophantine equation (3.9). So Hadano's conjecture is not true. □

Remark. In the case $k = 1$, we have the following example. Consider elliptic curve B_u with $u = 2$. This gives a sequence

$$\text{'550k3'} \to \text{'550k2'} \to \text{'550k1'}.$$

This curve corresponds to the solution $(r,s) = (125/2, -1/32)$ in the equation (3.8).

3.4 Proof of the main theorem

We need the following theorem of Dummigan.

Theorem 3.14 (Dummigan; Therem 1.2 in [Dum])**.** *Let $E \in \mathcal{C}$ be an elliptic curve defined over $\mathbf{Q}$ of square-free conductor N with a rational point of order $\ell \nmid N$. Then $E_0 \in \mathcal{C}$ has a rational point of order ℓ.*

Let f be the newform associated to an elliptic curve E of conductor N. Consider the case that N is square-free. For $d \mid N$, let W_d be the Atkin–Lehner involution and let $w_d = \pm 1$ be such that $W_d f = w_d f$ (cf. [AtLe]). We note that for primes $p \mid N$, $w_p = -1$ or $+1$ according as the multiplicative reduction at p is split or non-split, respectively.

Proposition 3.15. *Let E_0 be the $X_0(N)$-optimal curve of an isogeny class $\mathcal{C}$ of elliptic curves defined over $\mathbf{Q}$ of conductor N and ℓ be an odd prime. Suppose that N is square-free and $\ell \nmid N$. If $\mu_\ell \subset E_0[\ell]$, then there is only one prime $p \mid N$ such that $w_p = -1$.*

Proof. By Theorem 1.1 in [Vat], $\mu_\ell \subset E_0[\ell]$ must be contained in the Shimura subgroup $\Sigma(N)$ of $J_0(N)$. By Theorem 1 of [LiOe], $\Sigma(N)$ is isomorphic to a subgroup of $\mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, U)$, where U is the group of complex numbers of modulus 1. So μ_ℓ is isomorphic to a subgroup of $\mathrm{Hom}((\mathbf{Z}/p\mathbf{Z})^\times, U)$ for a prime $p \mid N$ such that $p \equiv 1 \pmod{\ell}$. We know that $w_p = -1$ because $p \equiv 1 \pmod{\ell}$ implies that E_0 has split multiplicative reduction at p. By Theorem 3 of [LiOe], W_p acts on μ_ℓ by multiplication -1 and W_q acts trivially on μ_ℓ for primes $q \neq p$ and $q \mid N$. This implies that $w_p = -1$ and $w_q = 1$ for primes $q \neq p$ and $q \mid N$. □

Proof of Theorem 3.8. The $\mathbf{Q}$-isogeny class of $X_0(11)$ consists of 3 elliptic curves '11a1' $= X_0(11)$, '11a2' $= X_0(11)/(\mathbf{Z}/5\mathbf{Z})$ and '11a3' $= X_0(11)/\mu_5 = X_1(11)$ (cf. Cremona's database [Cre]). So we have rational étale isogenies

$$\text{'11a3'} \longrightarrow \text{'11a1'} \longrightarrow \text{'11a2'}.$$

Hence $X_0(11)$- and $X_1(11)$-optimal curves differ by a 5-isogeny.

Now, let C be an isogeny class of elliptic curves over $\mathbf{Q}$ with a square-free conductor N which is not divisible by 5. Suppose that E_0 and E_1 differ by a 5-isogeny. Then by Vatsal's theorem (Theorem 3.5), there is an étale rational 5-isogeny $E_1 \longrightarrow E_0$. So E_1 contains a rational point of order 5. By Dummigan's theorem (Theorem 3.14), E_0 also contains a rational point of order 5 and by taking the quotient by the subgroup it generates, we can find another curve $E' \in C$. We know that E' has no rational 5-torsion points (cf. [Ken]). So we have the following diagram of curves and étale 5-isogenies:

$$E_1 \longrightarrow E_0 \longrightarrow E'.$$

As E_1 has a rational point of order 5, the curve E_1 has a Weierstrass equation of the form

$$y^2 + (v-u)xy - uv^2y = x^3 - uvx^2,$$

where $u, v \in \mathbf{Z}$ with $\gcd(u,v) = 1$. As we have assumed $5 \nmid N$, we can invoke Hadano's consideration (cf. §3.3) with $k = 0$. Since $w_p = -1$ for each prime p dividing uv, we must conclude that uv is divisible by *at most* one prime p, by Proposition 3.15. Suppose that $uv = \pm 1$. Invoking Hadano's consideration, our sequence of curves with étale isogenies $E_1 \longrightarrow E_0 \longrightarrow E'$ corresponds to finding a rational solution $(s,t) \in \mathbf{Q} \times \mathbf{Q}$ of equation (3.9) with an additional condition of $s = v/u = \pm 1$. Since the polynomial equation $t^4 + 5t^2 + 5$ does not admit rational solutions, we must have $t = 1$ and this solution gives $E_0 = X_0(11)$ and $E_1 = X_1(11)$.

Now, it remains to deal with the case $uv = \pm p$ for some prime p. Hadano's diophantine equation (3.9) in this case has the form

$$p^2 \pm p(t^4 + 5t^2 + 5)t = 1.$$

Changing this equation into a homogeneous form and viewing it mod p, we easily deduce that it does not admit a rational solution in $t \in \mathbf{Q}$. □

Chapter 4

Gross–Zagier conjecture

"From life's school of war: what does not kill me makes me stronger."

Friedrich Nietzsche,
Twilight of the Idols, or, How to Philosophize with a Hammer

4.1 Statement of the conjecture

The goal of this chapter is to prove a conjecture made by Gross and Zagier in [GrZa] concerning certain divisibility among arithmetic invariants of elliptic curves. This gives a theoretical evidence to the "strong form" of Birch and Swinnerton-Dyer conjecture 2.31, predicting that the leading coefficient of the Hasse–Weil L-function of an elliptic curve encodes some precise arithmetic invariants attached to the curve.

In [GrZa], Gross and Zagier gave a formula for the first derivative at $s = 1$ of the L-series of certain modular forms. In particular, they transferred the formula to the realm of L-functions of elliptic curves, under the modularity assumption (see Theorem 2.29). So let E be an elliptic curve defined over $\mathbf{Q}$ with conductor N. For

a negative square-free integer d, we consider the quadratic twist E_d of E which is in general *not* isomorphic to E over $\mathbf{Q}$ but becomes isomorphic over the imaginary quadratic field $K = \mathbf{Q}(\sqrt{d})$. We denote the discriminant of K over $\mathbf{Q}$ by $\mathrm{disc}(K)$ which is equal to d when $d \equiv 1 \pmod 4$ and to $4d$ otherwise. We also assume a close relation between E and K in such a way that each prime number dividing N splits completely in K. This is called the *Heegner condition* or *Heegner hypothesis* in the literature, which we assume throughout this chapter. The corresponding L-functions are also strongly related: we have $L(E/K, s) = L(E/\mathbf{Q}, s) \cdot L(E_d/\mathbf{Q}, s)$. By computing root numbers, the Heegner condition forces that $L(E/K, 1) = 0$. Throughout this chapter, we use the following notations.

- N is the conductor of E.
- ω is the *Néron differential* of E over $\mathbf{Q}$ and $\|\omega\|^2 := \int_{E(\mathbf{C})} |\omega \wedge \overline{\omega}|$ is the complex period.
- $P_K \in E(K)$ is the *Heegner point* over K. This depends on the elliptic curve and its modular parametrisation chosen.
- $2u_K$ is the number of roots of unity contained in the field K. $u_K = 1$ for all imaginary quadratic fields K except when $K = \mathbf{Q}(\sqrt{-1})$ and $K = \mathbf{Q}(\sqrt{-3})$, in these cases we have $u_K = 2$ and $u_K = 3$ respectively.
- C is the *Tamagawa number* of E over $\mathbf{Q}$ which is defined by the product $C = \prod_{p|N} C_p$ of all local Tamagawa numbers, where $C_p = [E(\mathbf{Q}_p) : E^0(\mathbf{Q}_p)]$.

Now the main theorem of Gross and Zagier ([GrZa], Theorem I.6.3) has the following consequence.

Theorem 4.1 ([GrZa], Theorem I.7.3 and V.2.1)**.** *Let $E/\mathbf{Q}$ be an elliptic curve of conductor N, and let K be an imaginary quadratic field satisfying the Heegner hypothesis. Assume that $L(E/K, 1) = 0$. Then,*

$$L'(E/K, 1) = \frac{\|\omega\|^2 \cdot \hat{h}(P_K)}{M^2 \cdot u_K^2 \cdot |\operatorname{disc}(K)|^{1/2}}. \tag{4.1}$$

In particular, $\operatorname{ord}_{s=1} L(E/K, s) = 1$ *if and only if P_K has infinite order.*

Assume that $\operatorname{ord}_{s=1} L(E/K, s) = 1$ here and thereafter (thus P_K has infinite order). Then the rank $r = \operatorname{rank} E(K)$ must be greater than or equal to 1. We invoke here Kolyvagin's amendment to the Gross–Zagier theorem.

Theorem 4.2 (Kolyvagin; Theorem 5 in [Kol])**.** *If* $\operatorname{ord}_{s=1} L(E/K, s) = 1$*, then* $r = 1$ *and* $Ш(E/K)$ *is finite.*

Now recall the Birch and Swinnerton-Dyer conjecture 2.31 for E over the imaginary quadratic field K.

Conjecture 4.3 (Birch and Swinnerton-Dyer)**.** If $\operatorname{ord}_{s=1} L(E/K, s) = 1$, then

$$L'(E/K, s) = \mathrm{BSD}_{E/K} = \frac{\#Ш(E/K) \cdot \mathrm{Reg}(E/K) \cdot C(E/K) \cdot \Omega(E/K)}{(\#E(K)_{\mathrm{tors}})^2 \cdot \sqrt{|\operatorname{disc}(K)|}} \tag{4.2}$$

(from Equation (2.11)).

Let us investigate the terms in the formula (4.2) more closely. First, we want to express $\mathrm{Reg}(E/K)$ in terms of $\hat{h}(P_K)$. We need to be careful because P_K need not be a generator for the 1-dimensional free part $E(K)/E(K)_{\mathrm{tors}}$. Put P to be a generator for $E(K)/E(K)_{\mathrm{tors}}$, and let $\nu = [\mathbf{Z}P : \mathbf{Z}P_K]$ (we call this quantity the *Heegner index* later). Note that

$$\frac{\mathrm{Reg}(E/K)}{(\#E(K)_{\mathrm{tors}})^2} = \frac{\hat{h}(P)}{[E(K) : \mathbf{Z}P]^2} = \frac{\hat{h}(P_K)}{\nu^2 [E(K) : \mathbf{Z}P]^2} = \frac{\hat{h}(P_K)}{[E(K) : \mathbf{Z}P_K]^2}.$$

The complex period $\Omega(E/K)$ is by definition

$$\Omega(E/K) = \int_{E(\mathbf{C})} |\omega|_{\mathbf{C}} = \int_{E(\mathbf{C})} |\omega \wedge \overline{\omega}| = \|\omega\|^2.$$

The product of Tamagawa numbers $C(E/K)$ can be expressed as

$$C(E/K) = \prod_{\mathfrak{p} \text{ bad}} [E(K_{\mathfrak{p}}) : E^0(K_{\mathfrak{p}})] = \prod_{p \mid N} [E(\mathbf{Q}_p) : E^0(\mathbf{Q}_p)]^2,$$

by considering Heegner hypothesis (any prime $p \mid N$ must split completely in K). For simplicity, we write $C_p := [E(\mathbf{Q}_p) : E^0(\mathbf{Q}_p)]$ and $C = \prod_{p \mid N} C_p$. Then we have

$C(E/K) = C^2$. Using these notations and conventions, we can restate the formula (4.2) as

$$\mathrm{BSD}_{E/K} = \frac{\#Ш(E/K) \cdot \hat{h}(P_K) \cdot C^2 \cdot \|\omega\|^2}{[E(K) : \mathbf{Z}P_K]^2 \cdot \sqrt{|\operatorname{disc}(K)|}}. \tag{4.3}$$

Equating the above two formulae (4.1) and (4.3), Gross and Zagier obtained the following conjecture.

Conjecture 4.4 (Strong Gross–Zagier Conjecture; [GrZa], Conjecture V.2.2)**.**

$$[E(K) : \mathbf{Z}P_K] = u_K \cdot C \cdot M \cdot (\#Ш(E/K))^{1/2}. \tag{4.4}$$

As the order of the rational torsion subgroup $E(\mathbf{Q})_{\mathrm{tors}}$ clearly divides the index $[E(K) : \mathbf{Z}P_K]$, they also obtained a weaker version of the conjecture, which we call "the Gross–Zagier conjecture" throughout this chapter.

Conjecture 4.5 (Weak Gross–Zagier Conjecture; [GrZa], Conjecture V.2.3)**.** The integer $u_K \cdot C \cdot M \cdot (\#Ш(E/K))^{1/2}$ is divisible by $\#E(\mathbf{Q})_{\mathrm{tors}}$.[1]

4.2 Previous results and Main theorem

Rational torsion subgroups of elliptic curves E over $\mathbf{Q}$ are completely classified by Mazur, see §2.3 or [Maz78]: $E(\mathbf{Q})_{\mathrm{tors}}$ is isomorphic to one of the following groups:

$$\begin{cases} \mathbf{Z}/n\mathbf{Z} & \text{for } 1 \leq n \leq 10,\ n = 12, \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z} & \text{for } n = 2, 4, 6, 8. \end{cases}$$

In [Lor], Lorenzini obtained the following theorem.

Theorem 4.6 ([Lor], Proposition 1.1)**.** *Let E be an elliptic curve defined over $\mathbf{Q}$ with a $\mathbf{Q}$-rational point of order k. Then the following statements hold.*[2]

(i) If $k = 4$, then $2 \mid C$, except for '15a7', '15a8', and '17a4'.

[1] Note that the order of $Ш(E/K)$ is finite due to Kolyvagin's theorem (see [Kol]), and that it follows that it is square by Cassels–Tate pairing (e.g. Theorem X.4.14 in [Sil09]).

[2] The exceptions are given by their labels in Cremona's table [Cre].

(ii) If $k = 5, 6,$ *or* 12, *then* $k \mid C$, *except for '11a3', '14a4', '14a6', and '20a2'.*

(iii) If $k = 7, 8,$ *or* 9, *then* $k^2 \mid C$, *except for '15a4', '21a3', '26b1', '42a1', '48a6', '54b3', and '102b1'.*

(iv) If $k = 10$, *then* $50 \mid C$.

Without exception, $k \mid C$ *if* $k = 7, 8, 9, 10$ *or* 12.

For the exceptions of above proposition, we can check that $\#E(\mathbf{Q})_{\mathrm{tors}}$ divides $C \cdot M$, except for '15a7', which is considered in §4.6. So the only remaining cases for the validity of the conjecture are those when $E(\mathbf{Q})_{\mathrm{tors}}$ is isomorphic to the following 4 groups: $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$, and $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$.

Among these remainders, when $E(\mathbf{Q})_{\mathrm{tors}}$ has a point of order 3, i.e., when $E(\mathbf{Q})_{\mathrm{tors}} \cong \mathbf{Z}/3\mathbf{Z}$ or $E(\mathbf{Q})_{\mathrm{tors}} \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$, the truth of Gross–Zagier conjecture was dealt by Byeon and Yhee in [BKY]. Our goal here is to prove yet remaining cases, thus to complete the proof of the conjecture.

Theorem 4.7 (Main theorem for Chapter 4)**.** *Let* E *be an elliptic curve defined over* $\mathbf{Q}$ *such that the rational torsion subgroup* $E(\mathbf{Q})_{\mathrm{tors}}$ *is isomorphic to one of the 4 groups:* $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$, *and* $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$. *Let* K *be an imaginary quadratic field such that* $E(K)$ *is of (analytic) rank 1 and that* K *satisfies the Heegner condition. Then the conjecture 4.5 is true, i.e.,* $\#E(\mathbf{Q})_{\mathrm{tors}}$ *divides* $C \cdot M \cdot u_k \cdot (\#Ш(E/K))^{1/2}$.

The proof will be given in a separated manner in §§ 4.4 – 4.7.

4.3 Preliminaries

4.3.1 Kramer's formula

In this subsection we introduce a formula of Kramer [Kra], and discuss how to measure the size of the Tate–Shafarevich group of elliptic curve making use of it. The purpose of this subsection is to provide a tool to show the main theorem for the cases $E(\mathbf{Q})_{\mathrm{tors}} \cong \mathbf{Z}/2\mathbf{Z}$ or $\mathbf{Z}/4\mathbf{Z}$. Thus, throughout this subsection, we assume $E(\mathbf{Q})_{\mathrm{tors}} \cong \mathbf{Z}/2\mathbf{Z}$ or $\mathbf{Z}/4\mathbf{Z}$, and consequently $E(\mathbf{Q})[2] \cong \mathbf{Z}/2\mathbf{Z}$.

Since the Tate–Shafarevich group $Ш(E/K)$ is finite (Theorem 5 in [Kol]), its 2-primary part $Ш(E/K)[2^\infty]$ has perfect square order. So if we find a non-trivial element in $Ш(E/K)[2]$, (or equivalently $\dim_{\mathbf{F}_2} Ш(E/K)[2] \geq 1$), we can immediately see that $2 \mid (\#Ш(E/K))^{1/2}$. So in this subsection, we are concentrating on how to find such a non-trivial element.

Let p be a prime number. We use the following notations.

- The *local norm index of E at p* is

$$i_p = \dim_{\mathbf{F}_2} \operatorname{coker} \mathrm{Norm}_{K_\mathfrak{p}/\mathbf{Q}_p} = \dim_{\mathbf{F}_2} E(\mathbf{Q}_p)/\mathrm{Norm}_{K_\mathfrak{p}/\mathbf{Q}_p} E(K_\mathfrak{p}),$$

  where $\mathrm{Norm}_{K_\mathfrak{p}/\mathbf{Q}_p} : E(K_\mathfrak{p}) \longrightarrow E(\mathbf{Q}_p)$ is the *norm map*.

- Let

$$\Phi = \left\{ \xi \in \mathrm{Sel}^2(E/\mathbf{Q}) : \xi \in \mathrm{Norm}_{K_\mathfrak{p}/\mathbf{Q}_p} \left(\prod_{\mathfrak{p}\mid p} \mathrm{Sel}^2(E/K_\mathfrak{p}) \right) \right\}.$$

  This group is called the *everywhere-local norm group*. Here $\mathrm{Sel}^2(E/K_\mathfrak{p})$ denotes the image of the group $E(K_\mathfrak{p})/2E(K_\mathfrak{p})$ in $H^1(K_\mathfrak{p}, E[2])$ (cf. §2.6).

- NS' is the image of the norm map $\mathrm{Sel}^2(E/K) \longrightarrow \mathrm{Sel}^2(E/\mathbf{Q})$, which we do not need in this paper.

Theorem 4.8 ([Kra], Theorem 1)**.** *The dimension of $Ш(E/K)[2]$ (over $\mathbf{F}_2$) is equal to*

$$\sum i_\ell + \dim_{\mathbf{F}_2} \Phi + \dim_{\mathbf{F}_2} NS' - \operatorname{rank} E(K) - 2\dim_{\mathbf{F}_2} E(\mathbf{Q})[2],$$

where the sum is taken over all primes (including infinity) of $\mathbf{Q}$.

Back to our case. Because $\operatorname{rank} E(K) = 1$ and $E(\mathbf{Q})[2] \cong \mathbf{Z}/2\mathbf{Z}$, by Theorem 4.8, $\dim_{\mathbf{F}_2} Ш(E/K)[2] \geq 1$ if and only if the quantity

$$\sum i_\ell + \dim_{\mathbf{F}_2} \Phi + \dim_{\mathbf{F}_2} NS'$$

is greater than or equal to 4.

Local norm indices

For general introduction and useful facts about the numbers i_ℓ, we refer to §4 of [Maz72b] and §2 of [Kra]. We only concern those numbers relevant to our situation. The proof of the following proposition can be found in §2 of [Kra].

Proposition 4.9. *Let E be an elliptic curve over $\mathbf{Q}$ with $E(\mathbf{Q})[2] \cong \mathbf{Z}/2\mathbf{Z}$, and with minimal discriminant $\Delta_{\min}$ and let $K = \mathbf{Q}(\sqrt{d})$ be an imaginary quadratic field satisfying the Heegner hypothesis. The local norm indices i_ℓ for various primes ℓ are given as follows.*

(i) *One has* $i_\infty = \begin{cases} 0 & \text{if } \Delta_{\min} < 0, \\ 1 & \text{if } \Delta_{\min} > 0. \end{cases}$

(ii) *Let p be an odd prime. If p is a good prime for E and is ramified in K, then one has $i_p = \dim_{\mathbf{F}_2} E[2](k)$, where k is the residue field of $\mathbf{Q}_p$. Otherwise one has $i_p = 0$.*

(iii) *If 2 is a good prime for E and is ramified in K, then one has*

$$i_2 = \begin{cases} 2 & \text{if } (\Delta_{\min}, d)_{\mathbf{Q}_2} = +1, \\ 1 & \text{if } (\Delta_{\min}, d)_{\mathbf{Q}_2} = -1, \end{cases}$$

where $(-,-)_{\mathbf{Q}_2}$ denotes the Hilbert norm-residue symbol. Otherwise, one has $i_2 = 0$.

Question 4.10. Can we find such formulae for i_ℓ for other cases?

Everywhere-local norm group

Now we provide a way to compute the everywhere-local norm group Φ. The following is the key.

Proposition 4.11 ([Kra], Proposition 7)**.** *The everywhere-local norm group Φ is the intersection of $\mathrm{Sel}^2(E/\mathbf{Q})$ and $\mathrm{Sel}^2(E_d/\mathbf{Q})$ inside $H^1(\mathbf{Q}, E[2]) \cong H^1(\mathbf{Q}, E_d[2])$, where E_d is the quadratic twist of E by d.*

Let E_d be the quadratic twist of E by d. In particular, suppose E is defined by the Weierstrass equation

$$y^2 = x^3 + Ax^2 + Bx, \tag{4.5}$$

which has discriminant $\Delta = 2^4B^2(A^2 - 4B)$. Then E_d has the Weierstrass equation of the form

$$y^2 = x^3 + Adx^2 + Bd^2x. \tag{4.6}$$

The discriminant of the above equation (4.6) is given by $\Delta_d = 16d^6B^2(A^2 - 4B)$.

Proposition 4.12. *The 2-torsion subgroups $E[2]$ and $E_d[2]$ are canonically isomorphic as $\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})$-modules. Consequently, the Galois cohomology groups $H^\bullet(\mathbf{Q}, E[2])$ and $H^\bullet(\mathbf{Q}, E_d[2])$ are isomorphic. In the sequel, we identify*

$$H^1(\mathbf{Q}, E[2]) = H^1(\mathbf{Q}, E_d[2]).$$

Proof. In terms of the equations (4.5) and (4.6), the Galois-equivariant isomorphism $E[2] \longrightarrow E_d[2]$ is given by $(t, 0) \longmapsto (dt, 0)$. □

Denote by P (resp. P_d) the rational torsion point of order 2 in E (resp. E_d) corresponding to $(0, 0)$ in Equation (4.5) (resp. $(0, 0)$ in Equation (4.6)). Let E' (resp. E'_d) be the elliptic curve $E/\langle P\rangle$ (resp. $E_d/\langle P_d\rangle$) and let ϕ (resp. ϕ_d) be the canonical quotient 2-isogeny $E \longrightarrow E'$ (resp. $E_d \longrightarrow E'_d$).

Proposition 4.13. *There are canonical homomorphisms*

$$H^1(\mathbf{Q}, E[\phi]) \longrightarrow H^1(\mathbf{Q}, E[2]), \quad \textit{and} \quad H^1(\mathbf{Q}, E_d[\phi_d]) \longrightarrow H^1(\mathbf{Q}, E_d[2]),$$

and they induce

$$\mathrm{Sel}^\phi(E/\mathbf{Q}) \longrightarrow \mathrm{Sel}^2(E/\mathbf{Q}), \quad \textit{and} \quad \mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q}) \longrightarrow \mathrm{Sel}^2(E_d/\mathbf{Q}).$$

Proof. If we denote the unique dual rational 2-isogeny of ϕ by ϕ', then we have a canonical exact sequence

$$0 \longrightarrow E[\phi] \longrightarrow E[2] \longrightarrow E'[\phi'] \longrightarrow 0. \tag{4.7}$$

This defines a canonical map $H^1(\mathbf{Q}, E[\phi]) \longrightarrow H^1(\mathbf{Q}, E[2])$ on cohomology groups, and it does restrict to $\mathrm{Sel}^\phi(E/\mathbf{Q})$ to give the map $\mathrm{Sel}^\phi(E/\mathbf{Q}) \longrightarrow \mathrm{Sel}^2(E/\mathbf{Q})$. For E_d and ϕ_d the proof is *mutatis mutandis* the same. □

Proposition 4.14. *There are canoncial isomorphisms*

$$H^1(\mathbf{Q}, E[\phi]) \cong \mathbf{Q}^\times/\mathbf{Q}^{\times 2} \quad \textit{and} \quad H^1(\mathbf{Q}, E_d[\phi_d]) \cong \mathbf{Q}^\times/\mathbf{Q}^{\times 2}.$$

Moreover, the isomorphisms are compatible in the sense that the following diagram is commutative:

$$\begin{array}{ccccc} & & H^1(\mathbf{Q}, E[\phi]) & \longrightarrow & H^1(\mathbf{Q}, E[2]) \\ & \overset{\sim}{\nearrow} & \downarrow & & \downarrow = \\ \mathbf{Q}^\times/\mathbf{Q}^{\times 2} \cong H^1(\mathbf{Q}, \mu_2) & & & & \\ & \underset{\sim}{\searrow} & & & \\ & & H^1(\mathbf{Q}, E_d[\phi_d]) & \longrightarrow & H^1(\mathbf{Q}, E_d[2]) \end{array}$$

where the vertical map in the middle is induced by the canonical isomorphism in the Proposition 4.12.

Proof. Clearly the isomorphisms $\mu_2 \longrightarrow E[\phi]$ and $\mu_2 \longrightarrow E_d[\phi_d]$ are compatible in the sense the left triangle of the diagram commutes. By Kummer theory we know $H^1(\mathbf{Q}, \mu_2) = \mathbf{Q}^\times/\mathbf{Q}^{\times 2}$, whence the result follows. □

Proposition 4.15. *Let G be the subgroup of $\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$ generated by the class of $A^2 - 4B$. Then G is the kernel of the homomorphisms $H^1(\mathbf{Q}, E[\phi]) \longrightarrow H^1(\mathbf{Q}, E[2])$ and $H^1(\mathbf{Q}, E_d[\phi_d]) \longrightarrow H^1(\mathbf{Q}, E_d[2])$. Thus,*

$$\ker\left(\mathrm{Sel}^\phi(E/\mathbf{Q}) \longrightarrow \mathrm{Sel}^2(E/\mathbf{Q})\right) = G \cap \mathrm{Sel}^\phi(E/\mathbf{Q}) \subset \mathrm{Sel}^\phi(E/\mathbf{Q}).$$

Similarly,

$$\ker\left(\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q}) \longrightarrow \mathrm{Sel}^2(E_d/\mathbf{Q})\right) = G \cap \mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q}) \subset \mathrm{Sel}^\phi(E_d/\mathbf{Q}).$$

Proof. We only give a proof for E and ϕ. For E_d and ϕ_d, everything is the same under making certain notational change. From the short exact sequence (4.7), we have the long exact sequence of cohomology groups:

$$\begin{aligned} 0 \longrightarrow E(\mathbf{Q})[\phi] \longrightarrow E(\mathbf{Q})[2] \longrightarrow E'(\mathbf{Q})[\phi'] & \\ \xrightarrow{\eta} H^1(\mathbf{Q}, E[\phi]) \longrightarrow H^1(\mathbf{Q}, E[2]) \longrightarrow H^1(\mathbf{Q}, E'[\phi']) \longrightarrow \cdots & \end{aligned}$$

Because we only consider those elliptic curves with $E(\mathbf{Q})[\phi] = E(\mathbf{Q})[2]$, the map $E(\mathbf{Q})[2] \longrightarrow E'(\mathbf{Q})[\phi']$ is the zero map, and this again forces us that $\eta : E'(\mathbf{Q})[\phi'] \longrightarrow H^1(\mathbf{Q}, E[\phi])$ is injective. The image $\eta\left(E'(\mathbf{Q})[\phi']\right)$ is the kernel of $H^1(\mathbf{Q}, E[\phi]) \longrightarrow H^1(\mathbf{Q}, E[2])$.

We claim that this kernel is equal to G. Write $E(\overline{\mathbf{Q}})[2] = \{O, P, Q, P+Q\}$, where O is the identity of E and $P \in E(\mathbf{Q})$, and similarly write $E'(\overline{\mathbf{Q}})[\phi'] = \{O', T\}$, where O' is the identity of E'. Clearly $T \in E'(\mathbf{Q})$. Since $E(\overline{\mathbf{Q}})[2] \longrightarrow E'(\overline{\mathbf{Q}})[\phi']$ is surjective but $E(\mathbf{Q})[2] \longrightarrow E'(\mathbf{Q})[\phi']$ is the zero map, the point Q is mapped onto T under $E(\overline{\mathbf{Q}})[2] \longrightarrow E'(\overline{\mathbf{Q}})[\phi']$. Then, $\eta(T) \in H^1(\mathbf{Q}, E[\phi])$ is defined by the 1-cocyle

$$\sigma \mapsto \sigma(Q) - Q = \begin{cases} P & \text{if } \sigma(Q) = P + Q \neq Q, \\ 0 & \text{if } \sigma(Q) = Q. \end{cases}$$

However, this 1-cocycle corresponds to the 1-cocycle $\sigma \mapsto \sigma(\sqrt{b})/\sqrt{b}$ defining an element $H^1(\mathbf{Q}, \mu_2)$, where $b = A^2 - 4B$, since in the Weierstrass equation (4.5), Q corresponds to one of the points $\left(\dfrac{-A \pm \sqrt{A^2-4B}}{2}, 0\right)$ and thus $\sigma(Q) = Q$ if and only if $\sigma\left(\sqrt{A^2-4B}\right) = \sqrt{A^2-4B}$. Clearly the 1-cocycle $\sigma \mapsto \dfrac{\sigma(\sqrt{A^2-4B})}{\sqrt{A^2-4B}}$ defining an element $H^1(\mathbf{Q}, \mu_2)$ corresponds to $A^2 - 4B$ in $\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$. □

Recall (Proposition 4.11) that the everywhere-local norm group Φ is the intersection of two Selmer groups $\mathrm{Sel}^2(E/\mathbf{Q})$ and $\mathrm{Sel}^2(E_d/\mathbf{Q})$ inside $H^1(\mathbf{Q}, E[2]) = H^1(\mathbf{Q}, E_d[2])$. In order to identify elements in the intersection, we need to find $b \in \mathbf{Q}^\times/\mathbf{Q}^{\times 2}$ such that $b \in \mathrm{Sel}^{\phi}(E/\mathbf{Q}) \cap \mathrm{Sel}^{\phi_d}(E/\mathbf{Q})$ by descent arguments (cf. [Sil09], chapter X). In order to ensure this is not the identity element in Φ, we should check $b \notin G$. This will be done when we deal with $E(\mathbf{Q})_{\mathrm{tors}} \cong \mathbf{Z}/4\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z}$.

4.3.2 Isogeny invariance of the Gross–Zagier conjecture

Let E and E' be isogenous elliptic curves defined over $\mathbf{Q}$, and K be an imaginary quadratic field satisfying the Heegner hypothesis. We consider those curves with fixed modular parametrisations $\pi : X_0(N) \longrightarrow E$ and $\pi' : X_0(N) \longrightarrow E'$.

Proposition 4.16. *Let $\theta : E \longrightarrow E'$ be a rational isogeny.*

(i) If the strong Gross–Zagier conjecture (Conjecture 4.4) is true for E then it is also true for E'.

(ii) Suppose that θ respects modular parametrisations of E and E', i.e., $\pi' = \theta \circ \pi$. Then we have

$$\frac{M^2 \cdot C^2 \cdot \#Ш(E/K)}{[E(K) : \mathbf{Z}P_K]^2} = \frac{M'^2 \cdot C'^2 \cdot \#Ш(E'/K)}{[E'(K) : \mathbf{Z}P'_K]^2}. \tag{4.8}$$

(iii) Let p be a prime. If

(a) $\operatorname{ord}_p \#E(K)_{\mathrm{tors}} = \operatorname{ord}_p \#E(\mathbf{Q})_{\mathrm{tors}}$, *and*

(b) $\operatorname{ord}_p \#E(\mathbf{Q})_{\mathrm{tors}} \leq \operatorname{ord}_p \left(u_K \cdot C \cdot M \cdot (\#Ш(E/K))^{1/2}\right)$,

then

$$\operatorname{ord}_p \#E'(\mathbf{Q})_{\mathrm{tors}} \leq \operatorname{ord}_p \left(u_K \cdot C' \cdot M' \cdot (\#Ш(E'/K))^{1/2}\right).$$

In particular, if $E(K)_{\mathrm{tors}} = E(\mathbf{Q})_{\mathrm{tors}}$, and if the weak Gross–Zagier conjecture (Conjecture 4.5) for E is true, then it is also true for E'.

Proof. (i) Isogenous curves E and E' have the same L-functions and the same BSD formulae, i.e., $L(E/K, s) = L(E'/K, s)$ and $\mathrm{BSD}_{E/K} = \mathrm{BSD}_{E'/K}$ (cf. Conjecture 2.31). The latter is a theorem of Cassels [Cas62]. As the strong Gross–Zagier conjecture is obtained by simply equating these formulae, it is clearly isogeny invariant.

(ii) Let P'_K be the Heegner point for E' defined by $P'_K = \theta(P_K)$. Since $L'(E/K, s) = L'(E'/K, s)$, we have

$$\frac{\|\omega\|^2 \cdot \hat{h}(P_K)}{\|\omega'\|^2 \cdot \hat{h}(P'_K)} = \frac{M^2}{M'^2}.$$

Similarly, from $\mathrm{BSD}_{E/K} = \mathrm{BSD}_{E'/K}$, we get

$$\frac{\|\omega\|^2 \cdot \hat{h}(P_K)}{\|\omega'\|^2 \cdot \hat{h}(P'_K)} = \frac{\#Ш(E'/K) \cdot C'^2 \cdot [E(K) : \mathbf{Z}P_K]^2}{\#Ш(E/K) \cdot C^2 \cdot [E'(K) : \mathbf{Z}P'_K]^2}.$$

Equating, we obtain the equation 4.8.

(iii) Let P (resp. P') be a generator of the group

$$E(K)/E(K)_{\mathrm{tors}} \quad (\text{resp. } E'(K)/E'(K)_{\mathrm{tors}}),$$

and let $P_K = \nu P$ (resp. $P'_K = \nu' P'$). As $P'_K = \theta(P_K) = \nu\theta(P)$, the index ν' is divisible by ν. The assumption (i) $\mathrm{ord}_p \#E(K)_{\mathrm{tors}} = \mathrm{ord}_p \#E(\mathbf{Q})_{\mathrm{tors}}$ implies that $\mathrm{ord}_p[E(K)_{\mathrm{tors}} : E(\mathbf{Q})_{\mathrm{tors}}] = 0$. By the equation 4.8, we have

$$\frac{u_K^2 \cdot M^2 \cdot C^2 \cdot \#Ш(E/K)}{(\#E(\mathbf{Q})_{\mathrm{tors}})^2 \cdot [E(K)_{\mathrm{tors}} : E(\mathbf{Q})_{\mathrm{tors}}]^2} = \frac{u_K^2 \cdot M'^2 \cdot C'^2 \cdot \#Ш(E'/K)}{\left(\frac{\nu'}{\nu}\right)^2 \cdot (\#E'(\mathbf{Q})_{\mathrm{tors}})^2 \cdot [E'(K)_{\mathrm{tors}} : E'(\mathbf{Q})_{\mathrm{tors}}]^2},$$

and by the assumption (ii) the left hand side of the above equation is a p-adic integer. Thus,

$$\begin{aligned} &\mathrm{ord}_p \left(u_K \cdot C' \cdot M' \cdot (\#Ш(E'/K))^{1/2} \right) \\ &\geq \mathrm{ord}_p \left(\frac{\nu'}{\nu} \cdot (\#E'(\mathbf{Q})_{\mathrm{tors}}) \cdot [E'(K)_{\mathrm{tors}} : E'(\mathbf{Q})_{\mathrm{tors}}] \right) \\ &\geq \mathrm{ord}_p \#E'(\mathbf{Q})_{\mathrm{tors}}. \end{aligned}$$

□

Remark. By [GJTo] Corollary 4 or [Naj], Theorem 2, for a given elliptic curve E defined over $\mathbf{Q}$, there are at most 4 quadratic fields K such that $E(K)_{\mathrm{tors}} \neq E(\mathbf{Q})_{\mathrm{tors}}$.

4.4 $E(\mathbf{Q})_{\mathrm{tors}} \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$

In this section, we prove the Main Theorem for the cases when $E(\mathbf{Q})_{\mathrm{tors}}$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$.

Theorem 4.17. *Suppose that $E(\mathbf{Q})_{\mathrm{tors}}$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$. Then the order $8 = \#E(\mathbf{Q})_{\mathrm{tors}}$ divides the Tamagawa number C of E, except for the curve '15a3', in which case $C \cdot M = 8$.*

From [Kub], table 3, such elliptic curves can be parametrised by one parameter $\lambda \in \mathbf{Q}$ by

$$y^2 + xy - \lambda y = x^3 - \lambda x^2, \tag{4.9}$$

where $\lambda = \left(\frac{\alpha}{\beta}\right)^2 - \frac{1}{16} = \frac{16\alpha^2 - \beta^2}{16\beta^2}$, with positive integers α, β having no common prime divisor, and $\alpha/\beta \neq 1/4$. The discriminant of the equation is $\Delta = \lambda^4(1+16\lambda) \neq 0$. Note that since we take α and β relatively prime, there are no common prime divisor of $16\alpha^2 - \beta^2$ and $16\beta^2$ except 2.

Proposition 4.18. *Let p be a prime.*

(i) If $m := \mathrm{ord}_p\, \lambda > 0$, then the reduction of E modulo p is (split) multiplicative of type I_{4m}. Consequently the Tamagawa number at p of E is $C_p = 4m$.

(ii) Suppose that $p \neq 2$. If $m := \mathrm{ord}_p\, \lambda < 0$, then m is always even, and the minimal Weierstrass equation at p is given by

$$y^2 + p^z xy - up^z y = x^3 - ux^2, \tag{4.10}$$

where $u \in \mathbf{Z}_p^\times$ satisfying $\lambda = up^m$ in $\mathbf{Z}_p$, and where z is a positive integer. The reduction type of the equation modulo p is I_n with $n = 2z$, whence $C_p = 2z$.

Proof. (i) This can be shown by directly applying Tate's algorithm (see [Sil94], §IV.9) to the Weierstrass equation (4.9).

(ii) Since $\gcd\left(16\alpha^2 - \beta^2, 16\beta^2\right)$ is a power of 2, if

$$m = \mathrm{ord}_p\, \lambda = \mathrm{ord}_p\left((16\alpha^2 - \beta^2)/16\beta^2\right) < 0$$

then the exponent m is always even. Changing Weierstrass equation (cf. [Lor], proof of Proposition 2.4), we get the equation (4.10). We use Tate's algorithm again for this equation to obtain the minimality and reduction type. □

Let

$$S = \left\{p \text{ primes} : \mathrm{ord}_p\, \lambda > 0\right\}, \qquad T = \left\{p \text{ primes} : p \neq 2,\ \mathrm{ord}_p\, \lambda < 0\right\}.$$

Proposition 4.18 says that Theorem 4.17 is true when (i) $\#S \geq 2$; or (ii) $\#S = 1$ and $\#T \geq 1$. Thus the following proposition shows Theorem 4.17.

Proposition 4.19. *With possible finite number of exceptions, we have* $\#S \geq 1$ *and moreover if* $T = \emptyset$*, then* $\#S \geq 2$*. The exceptions are exactly the following curves: '15a1', '15a3', '21a1', '24a1', '48a3', '120a2', '240a3', '240d5', and '336e4'. But in any case including these exceptions, we have* $8 \mid C \cdot M$*.*

Proof. Write $\beta = 2^n\beta'$ with $n \geq 0$ and β' odd. The condition $T = \emptyset$ is equivalent to the condition $\beta' = 1$. We divide the proof according to the value of n.

Suppose $n = 0$. In this case $16\alpha^2 - \beta^2$ is odd and so $\gcd\left(16\alpha^2 - \beta^2, 16\beta^2\right) = 1$. Suppose that there is no prime dividing $16\alpha^2 - \beta^2$. We then have $16\alpha^2 - \beta^2 = \pm 1$. This is possible only if $\alpha = 0$, a contradiction. For the second statement, assume $\beta = 1$. In this case, we get $\lambda = (16\alpha^2 - 1)/16$. If there is only one odd prime p dividing $16\alpha^2 - 1$, then we must have $4\alpha - 1 = 1$, a contradiction ($\alpha \in \mathbf{Z}_{>0}$).

Suppose $n = 1$. We have

$$\lambda = \frac{16\alpha^2 - 4\beta'^2}{16 \cdot 4\beta'^2} = \frac{4\alpha^2 - \beta'^2}{16\beta'^2},$$

and $\gcd\left(4\alpha^2 - \beta'^2, 16\beta'^2\right) = 1$. If there were no odd prime dividing $4\alpha^2 - \beta'^2$, we would have $4\alpha^2 - \beta'^2 = \pm 1$, whence $\alpha = 0$, a contradiction. If $\beta = 2$ (equivalently $\beta' = 1$), and if there were only one prime dividing $4\alpha^2 - \beta'^2$, then either one of the relations $2\alpha - 1 = 1$ or $2\alpha + 1 = -1$ would hold. Thus we must have $\alpha = 1$. In this case we get the curve '48a3', having $C_2 = C_3 = 4$.

Suppose $n = 2$. We have

$$\lambda = \frac{16\alpha^2 - 16\beta'^2}{16 \cdot 16\beta'^2} = \frac{\alpha^2 - \beta'^2}{16\beta'^2}/$$

As $\alpha^2 - \beta'^2 \equiv 0 \pmod 8$, if there were no prime dividing $\alpha^2 - \beta'^2$, we would have either one of the following: $\alpha^2 - \beta'^2 = \pm 8$, or $\alpha^2 - \beta'^2 = \pm 16$.

- Suppose $\alpha^2 - \beta'^2 = 8$. The only solution to this equation is $(\alpha, \beta') = (3, 1)$. This corresponds to $\lambda = 1/2$ and the curve '24a1', having $C_2 = 4$ and $C_3 = 2$.

- Suppose $\alpha^2 - \beta'^2 = -8$. The only solution to this equation is $(\alpha, \beta') = (1, 3)$. This corresponds to $\lambda = -1/18$ and the curve '24a1' again.

- Suppose $\alpha^2 - \beta'^2 = 16$. The only solution to this equation is $(\alpha, \beta') = (5, 3)$. This corresponds to $\lambda = 1/9$ and the curve '15a3', having $C_3 = 2$ and $C_5 = 2$. This is the exceptional case, but we also have $M = 2$ in this case, so the validity of Gross–Zagier conjecture stays unharmed.

- Suppose $\alpha^2 - \beta'^2 = -16$. The only solution to this equation is $(\alpha, \beta') = (3, 5)$. This corresponds to $\lambda = -1/25$ and the curve '15a3' again.

For the second statement, assume $\beta' = 1$, i.e., $\beta = 4$, and $\lambda = (\alpha^2 - 1)/16$. The only possible way for $\alpha^2 - 1$ to be a power of 2 is to have $\alpha = 3$, and this corresponds to '24a1' which we have dealt with before. So assume there is one and only one *odd* prime p dividing $\alpha^2 - 1$.

- Suppose that $\mathrm{ord}_2(\alpha^2 - 1) = 3$, i.e., $\alpha^2 - 1 = 8p^m$. We can see that the only possible solution to this equation is $\alpha = 5$, $p = 3$, and $m = 1$. The corresponding curve is '120a2', having $C_2 = C_3 = 4$ and $C_5 = 2$.

- Suppose that $\mathrm{ord}_2(\alpha^2 - 1) = 4$, i.e., $\alpha^2 - 1 = 16p^m$. As above, we can see that the solutions to the equation are $(\alpha, p, m) = (7, 3, 1)$ and $(9, 5, 1)$. The solution $(7, 3, 1)$ corresponds to '21a1' having $C_3 = 4$ and $C_7 = 2$, while $(9, 5, 1)$ does to '15a1' having $C_3 = 2$ and $C_5 = 4$.

- If $\mathrm{ord}_2(\alpha^2 - 1) \geq 5$, then $\mathrm{ord}_2 \lambda > 0$ as well as $\mathrm{ord}_p \lambda > 0$. So there always are more than two prime divisors in the numerator of λ.

Suppose $n \geq 3$. We have

$$\lambda = \frac{16\alpha^2 - 2^{2n}\beta'^2}{16 \cdot 2^{2n}\beta'^2} = \frac{\alpha^2 - 2^{2n-4}\beta'^2}{2^{2n}\beta'^2}.$$

Notice that $\gcd(\alpha^2 - 2^{2n-4}\beta'^2, 2^{2n}\beta'^2) = 1$. If there is no odd prime dividing the numerator, then we must have $\alpha^2 - 2^{2n-4}\beta'^2 = \pm 1$. By factoring the equation, we have the solutions $\alpha = \pm 1$ and $\beta' = 0$, which are absurd.

Suppose $T = \emptyset$, i.e., $\beta = 2^n$.

- Suppose $n = 3$, i.e., $\beta = 8$. In this case $\lambda = (\alpha^2 - 4)/64$. If there is only one prime p (necessarily odd) dividing $\alpha^2 - 4$, then by factoring, we must have

either $\alpha = 1$ or $\alpha = 3$. We cannot have $\alpha = 1$ because this corresponds to a singular curve ($\lambda = -1/16$). The case $\alpha = 3$ corresponds to the curve '240a3', having $C_2 = C_5 = 4$ and $C_3 = 2$.

- Suppose $n = 4$, i.e., $\beta = 16$. In this case $\lambda = (\alpha^2 - 16)/256$. If there is only one prime p (necessarily odd) dividing $\alpha^2 - 16$, then $\alpha = 3$ or $\alpha = 5$. The case $\alpha = 3$ corresponds to the curve '336e4', having $C_2 = C_7 = 4$ and $C_3 = 2$. If $\alpha = 5$, then we have '240d5', having Tamagawa numbers $C_2 = 4$, $C_3 = 8$, and $C_5 = 2$.

- Suppose $n \geq 5$. In this case we can take another Weierstrass equation (cf. Equation (4.10)) of E of the following form:

$$y^2 + 2^n xy - 2^n uy = x^3 - ux^2, \tag{4.11}$$

where $u = \alpha^2 - 2^{2n-4}$. This equation has discriminant $\Delta = (2^{2n} + 16u)2^{2n}u^4$ and $c_4 = 2^{2n+4}u + 16u^2 + 2^{4n}$, so $\mathrm{ord}_2(\Delta) = 2n + 4$ and $\mathrm{ord}_2(c_4) = 4$. Moreover, by [Sil09], Proposition VII.5.5, since its j-invariant has order $8 - 2n < 0$, E has potentially multiplicative reduction modulo 2. If this equation (4.11) is minimal at the prime 2, then the curve has additive reduction modulo 2 ($\mathrm{ord}_2(c_4) > 0$). Tate's algorithm says that E has reduction of type I_k^* for some k, with Tamagawa number 2 or 4. Suppose that the equation (4.11) is not minimal modulo 2. Then we can transform (4.11) into a minimal model modulo 2, which has discriminant of order $2n + 4 - 12 = 2n - 8$ at 2 and c_4 of order 0. Since the order of the minimal discriminant is even and > 0, and since E has multiplicative reduction ($\mathrm{ord}_2 c_4 = 0$), we have even C_2 by Tate's algorithm. As C_2 is even and $4 \mid C_p$ for some odd $p \in S$, the proof of this case is completed.

□

4.5 $E(\mathbf{Q})_{\mathrm{tors}} \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$

In this section, we prove the Main Theorem for the cases when $E(\mathbf{Q})_{\mathrm{tors}}$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.

Theorem 4.20. *Suppose that $E(\mathbf{Q})_{\mathrm{tors}}$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$. Then the order $4 = \#E(\mathbf{Q})_{\mathrm{tors}}$ divides the Tamagawa number C of E, except for two curves '17a2' and '32a2'. For these two cases we have $4 = C \cdot M$.*

Following [Kub], we can take a Weierstrass model of the form

$$y^2 = x(x+a)(x+b), \tag{4.12}$$

where $a, b \in \mathbf{Z}$ with $a \neq b \neq 0 \neq a$. Note that a and b is in general not relatively prime. The discriminant of the equation (4.12) is $\Delta = 16(a-b)^2a^2b^2$ and $c_4 = 16a^2 - 16ab + 16b^2$. Let $c = a - b \neq 0$. If there is a prime p dividing both a and b, then by changing the equation via $[p, 0, 0, 0]$ if necessary, we assume $\min\left(\mathrm{ord}_p\, a, \mathrm{ord}_p\, b\right) = 1$.

We first investigate the Tamagawa number C_p for primes p dividing abc.

Proposition 4.21. *Let p be a prime. Assume that either (a) $p \mid a$ and $p \nmid bc$; or (b) $p \mid b$ and $p \nmid ac$. Then we have the following.*

(i) If p is odd, then E has reduction of type $\mathrm{I}_{\mathrm{ord}_p \Delta} = \mathrm{I}_{2\,\mathrm{ord}_p(a)}$ modulo p, with even Tamagawa number at p.

(ii) Suppose that $p = 2$. If $m := \mathrm{ord}_2\, a = 4$ and if $b \equiv 1 \pmod 4$, then E has good reduction modulo 2, whence $C_2 = 1$. Otherwise, C_2 is even.

Proof. We only give the proof for the case (a). By the symmetry of the roles of a and b in the equation, the case (b) follows immediately.

(i) This is immediate from Tate's algorithm.

(ii) Suppose that $2 \mid a$ and $2 \nmid bc$. We do a case-by-case study. In order to help readers to re-construct proofs of the results in the following table, we remark that we mostly apply Tate's algorithm to the Weierstrass equation (4.12), while for the case $m = 4$ and $b \equiv 1 \pmod 4$ and for $m \geq 5$, we apply the algorithm to another Weierstrass equation $y^2 + xy = x^3 + \dfrac{a+b-1}{4}x^2 + \dfrac{ab}{2^4}x$.

m	$b \mod 4$	Reduction Type of E at $p=2$	C_2
1	1 or 3	III	2
2	1	I_n^*	2 or 4
	3	I_0^*	2
3	1	III^*	2
	3	I_n^*	2 or 4
4	1	I_0 (good)	1
	3	I_n^*	2 or 4
≥ 5	1 or 3	I_{2m-8}	even

□

Proposition 4.22. *Let p be a prime such that $p \mid c$ and $p \nmid ab$.*

(i) If p is odd, then E has reduction of type $\mathrm{I}_{\mathrm{ord}_p \Delta} = \mathrm{I}_{2\,\mathrm{ord}_p(c)}$ modulo p, with even Tamagawa number at p.

(ii) Suppose that $p = 2$. If $m := \mathrm{ord}_2 c = 4$ and if $a \equiv b \equiv 3 \pmod 4$, then E has good reduction modulo 2, whence $C_2 = 1$. Otherwise, C_2 is even.

Proof. We make a change of variables via $[1, -a, 0, 0]$, to get another equation

$$y^2 = x^3 + (-2a + b)x^2 + a(a - b)x. \tag{4.13}$$

(i) Immediate from Tate's algorithm applied to equation (4.13).

(ii) Let $p = 2$. Similar as above proposition, the results from Tate's algorithm applied to the equation (4.13) or to $y^2 + xy = x^3 + \dfrac{-2c - b - 1}{4}x^2 + \dfrac{ac}{16}x$ when dealing with the cases $a \equiv b \equiv 3 \pmod 4$ and $m \geq 4$, are summarised as follows.

- Suppose that $m := \mathrm{ord}_2 c = 1$. Then E has reduction of type III at 2, with Tamagawa number $C_2 = 2$.
- Suppose that $m = 2$ or 3 and $a \equiv b \equiv 3 \pmod 4$. Then E has reduction of type III^* at 2, with Tamagawa number $C_2 = 2$.
- Suppose that $m = 4$ and $a \equiv b \equiv 3 \pmod 4$. Then E has reduction of type I_0 (good reduction) at 2, with Tamagawa number $C_2 = 1$.

- Suppose that $m \geq 5$ and $a \equiv b \equiv 3 \pmod 4$. Then E has reduction of type I_{2m-8} at 2, with even Tamagawa number at 2.
- If $m \geq 2$ and either $a \equiv 1 \pmod 4$ or $b \equiv 1 \pmod 4$ (or both), then E has reduction of type I_k^* for some k at 2, with Tamagawa number $C_2 = 2$ or 4.

□

Proposition 4.23. *Let p be a prime dividing two of a, b, or c. Then clearly it divides the third. By changing variables in the equation* (4.12) *via* $[p, 0, 0, 0]$ *if necessary, we assume* $\min\left(\mathrm{ord}_p\, a, \mathrm{ord}_p\, b\right) = 1$. *Then E has reduction of type I_k^* for some k, with even Tamagawa number.*

Proof. If $m \neq n$, then we may assume $m > n = 1$ without any loss of generality. By Tate's algorithm, in this case E has reduction of type I_k^* with Tamagawa number 2 or 4. If $m = n = 1$, then we can write $a = pa'$ and $b = pb'$ with $(a', p) = (b', p) = 1$. Hence,

- if $a' \not\equiv b' \pmod p$, then E has reduction of type I_0^* modulo p with Tamagawa number 4;
- if $a' \equiv b' \pmod p$, then E has reduction of type I_k^* modulo p with Tamagawa number 2 or 4.

□

Recall that E is an elliptic curve defined by the equation $y^2 = x(x+a)(x+b)$ with discriminant $\Delta = 16a^2b^2c^2 \neq 0$ where $a, b, c := a - b \in \mathbf{Z}$. We also have assumed that $\min\left(\mathrm{ord}_p\, a, \mathrm{ord}_p\, b\right) \leq 1$ for all primes p. Let

$$S := \left\{p \text{ primes} : \mathrm{ord}_p\, a > 0,\ \mathrm{ord}_p\, b > 0\right\}.$$

If $\#S \geq 2$, then by Proposition 4.23, then the Tamagawa number C of E is divisible by 4. Thus the following proposition shows Theorem 4.20.

Proposition 4.24. *Suppose that $\#S \leq 1$. Then $4 \mid C$ with only two exceptions: '17a2' and '32a2'. But in both exceptions, we have $C = M = 2$.*

Proof. **Case 1**. $S = \{2\}$. We have even C_2. In addition, we may assume that abc is a power of 2, since the existence of odd prime divisor of abc immediately implies by Proposition 4.21 and Proposition 4.22, that C is divisible by 4. Suppose first that $\operatorname{ord}_2 a = \operatorname{ord}_2 b = 1$. Since $a \neq b$, then we may assume $a = 2$ and $b = -2$. This yields the curve '64a1', having $C_2 = 4$. Now, we assume $\operatorname{ord}_2 a \neq \operatorname{ord}_2 b$. Without loss of generality, assume $m := \operatorname{ord}_2 a > \operatorname{ord}_2 b = 1$. So $b = \pm 2$. Assume $b = 2$. Since $c = a - b = \pm 2^m - 2$ is also divisible only by 2, we must have $a = 4$. This again yields the curve '64a1', having Tamagawa number 4. For similar reasons, if $b = -2$, then we must have $a = -4$. This yields the same.

Case 2. $S = \{p\}$ for some odd prime p. We have even C_p. In this case, abc does not have any other odd prime factor except for p.

Suppose moreover that $2 \nmid ab$. Since $c = a - b$ must be even, so to avoid even C_2, we must assume that E has good reduction modulo 2, i.e., $\operatorname{ord}_2 c = 4$ and $a \equiv b \equiv 3 \pmod 4$, cf. Proposition 4.22. If $\operatorname{ord}_p a = \operatorname{ord}_p b = 1$, then since $a \equiv b \pmod 4$, we must have $a = b = \pm p$. But these only define singular curves. Hence assume $m := \operatorname{ord}_p a > \operatorname{ord}_p b = 1$, i.e., $a = \pm p^m$ and $b = \pm p$. Since $c = a - b = \pm p^m \pm p$ has to contain no prime factors other than 2 and p, and moreover the exponent of 2 in the prime decomposition of c has to be 4 by assumption, the only case this can occur is when $p = 17$ and $m = 2$. Then we have either $a = 17^2$ and $b = 17$ or $a = -17^2$ and $b = -17$. For these cases, we have elliptic curves '4624e2' and '289a2' respectively, and they have Tamagawa numbers divisible by 4.

Suppose either $2 \mid a$ or $2 \mid b$ (not both, of course) and E has good reduction modulo 2. Without loss of generality we assume $2 \mid a$, whence $\operatorname{ord}_2 a = 4$ with $b \equiv 1 \pmod 4$. Suppose first that $\operatorname{ord}_p a = \operatorname{ord}_p b = 1$. In this case we get $a = \pm 2^4 p$ and $b = \pm p$, whence $c = a - b = \pm 2^4 p \pm p = \pm 3 \cdot 5 \cdot p$ or $\pm 17 \cdot p$. Hence the only remaining cases are those when $p = 17$. Since $b \equiv 1 \pmod 4$, we must have $b = 17$, then we must pick $a = -2^4 \cdot 17$. This gives the curve '289a2', having Tamagawa number 4. Now, assume that $m := \operatorname{ord}_p a > \operatorname{ord}_p b = 1$. Then $a = \pm 2^4 p^m$ and $b = \pm p$, and thus we get $c = a - b = \pm 2^4 p^m \pm p = p(\pm 2^4 p^{m-1} \pm 1)$. However, in this case, c must have odd prime divisor other than p, so we do not need to concern this case. On the other hand, if we assume $m := \operatorname{ord}_p b > \operatorname{ord}_p a = 1$, then $a = \pm 2^4 p$ and $b = \pm p^m$. Since $c = \pm 2^4 p \pm p^m = p(\pm 16 \pm p^{m-1})$, we must have $p = 17$ and $m = 2$. In order to have

$b \equiv 1 \pmod 4$, we must pick $b = 17^2$, and $a = 16 \cdot 17$. This again gives us the curve '289a2'.

Case 3. $S = \emptyset$.

Suppose first that $2 \mid ab$.

1. E has bad reduction modulo 2, i.e., we have even C_2. Then $|abc|$ is a power of 2, in order to avoid $4 \mid C$. The only possible cases are $(a, b, c) = (2, 1, 1)$ or $(a, b, c) = (-2, -1, -1)$, and in either case the curve is '32a2', having $C = M = 2$.

2. E does have good reduction modulo 2, i.e., $C_2 = 1$. Then $\mathrm{ord}_2\, a = 4$ and $b \equiv 1 \pmod 4$.

   2.1. If $\{p \text{ primes} : p \neq 2,\ p \mid ab\} = \emptyset$, then $a = \pm 16$ and $b = 1$.

      2.1.1. If $a = 16$ and $b = 1$, then $c = 3 \cdot 5$ and we have even C_3 and C_5.

      2.1.2. If $a = -16$ and $b = 1$, then $c = -17$. In this case the curve is '17a2', having $C = M = 2$.

   2.2. Let p be an odd prime dividing ab.

      2.2.1. If $p \mid a$, then $a = \pm 16p^m$, $b = 1$, and $abc = 16p^m(16p^m \pm 1)$. Hence there are at least two odd primes dividing abc, making $4 \mid C$.

      2.2.2. If $p \mid b$, then $a = \pm 16$, $b = \pm p^m \equiv 1 \pmod 4$, and in order for p to be the unique odd prime dividing abc, we must have $(a, b, c) = (16, 17, -1)$, which yields the curve '17a2', having $C = M = 2$.

Suppose that $2 \nmid ab$. This means that c is always even.

1. E has bad reduction modulo 2, i.e., we have even C_2. In order to avoid $4 \mid C$, we must have $(a, b, c) = (1, -1, 2)$ or $(-1, 1, -2)$. In either case the resulting curve is '32a2', having $C = M = 2$.

2. E has good reduction modulo 2, i.e., $C_2 = 1$. Then $\mathrm{ord}_2\, c = 4$ and $a \equiv b \equiv 3 \pmod 4$.

   2.1. $\{p \text{ primes} : p \neq 2,\ p \mid ab\} = \emptyset$; this cannot be possible.

2.2. $\#\{p \text{ primes} : p \neq 2,\ p \mid ab\} = 1$, say p. Then we must have $(a, b, c) = (-1, -17, 16)$ or $(-17, -1, -16)$. In either case we have '17a2', having $C = M = 2$.

2.3. $\#\{p \text{ primes} : p \neq 2,\ p \mid ab\} \geq 2$; we always have $4 \mid C$.

□

4.6 $E(\mathbf{Q})_{\text{tors}} \cong \mathbf{Z}/4\mathbf{Z}$

Theorem 4.25. *If E is an elliptic curve defined over $\mathbf{Q}$, having rational torsion subgroup $E(\mathbf{Q})_{\text{tors}}$ isomorphic to $\mathbf{Z}/4\mathbf{Z}$, then the order $4 = \#E(\mathbf{Q})_{\text{tors}}$ divides $u_K \cdot C \cdot M \cdot (\#Ш(E/K))^{1/2}$.*

4.6.1 Tamagawa numbers

In order to prove Theorem 4.25, we first consider Tamagawa numbers of E.

From [Kub], table 3, such elliptic curves can be parametrized by one parameter λ by

$$y^2 + xy - \lambda y = x^3 - \lambda x^2,$$

where the discriminant of the equation $\lambda^4(1 + 16\lambda) \neq 0$. This is the same as in section 4.4, but without further restriction on λ. Let $\lambda = \alpha/\beta$, with $\alpha, \beta \in \mathbf{Z}$ and $\gcd(\alpha, \beta) = 1$. By Proposition 4.18 (a), we may assume $\alpha = 1$. So we begin with the following Weierstrass equation

$$y^2 + \beta xy - \beta^2 y = x^3 - \beta x^2, \tag{4.14}$$

with $\beta \in \mathbf{Z}$. Note that this curve has discriminant $\Delta = (16+\beta)\beta^7$ and $c_4 = (16+16\beta+\beta^2)\beta^2$. If $\beta = \pm 1$, then we have either '15a8' or '17a4', both of which have $M = 4$. So we may assume that there is at least one prime dividing β.

Let p be a prime dividing β, and let $m := \text{ord}_p \beta > 0$. Write $\beta = p^m u$, for some $u \in \mathbf{Z}$ with $\gcd(u, p) = 1$. Using Tate's algorithm applied to Weierstrass equations $y^2 + p^{z+1}xy - p^{z+2}u^{-1}y = x^3 - pu^{-1}x^2$ (when $m = 2z + 1$ is odd) or

$y^2 + p^{z+1}xy - p^{z+2}u^{-1}y = x^3 - pu^{-1}x^2$ (when $m = 2z$ is even), we can figure out the reduction types and Tamagawa numbers at primes $p \mid \beta$ for E.

m	p	conditions	$E \bmod p$	C_p
$m = 2z+1$ for $z \in \mathbf{Z}_{\geq 0}$	any		I_1^*	4
$m = 2z$ for $z \in \mathbf{Z}_{>0}$	$p \neq 2$		I_{2z}	even
	$p = 2$	$u \equiv 3 \pmod 4$ & $m = 8$	I_0 (good)	1
		otherwise	bad	even

So, in the sequel, we assume

- $\mathrm{ord}_p\, \beta$ is even for all prime p;
- the number of odd primes dividing β is ≤ 1.

Moreover, if ℓ is an odd prime dividing $\beta + 16$, then E has reduction of type $I_{\mathrm{ord}_\ell(\beta+16)}$ at ℓ.[3] We furthermore assume throughout this section, that

- if ℓ is an odd prime dividing $\beta + 16$, then $\mathrm{ord}_\ell\,(\beta + 16)$ is odd.

Suppose that there is no odd prime p dividing β, i.e., $\beta = \pm 2^m$ for some positive integer m. As we can see in the above table, in order to avoid $4 \mid C$, we may assume $m = 2z$ is even. Applying Tate's algorithm to the Weierstrass equation (4.14), we have the following results.

β	Curve	C	M
2^2	'40a3'	$C_2 \cdot C_5 = 2 \cdot 1$	2
2^4	'32a4'	$C_2 = 2$	2
2^{2z} with $z \geq 3$		$C_2 = 4$	
-2^2	'24a4'	$C_2 \cdot C_3 = 2 \cdot 1$	2
-2^4	singular curve		
-2^6	'24a3'	$C_2 \cdot C_3 = 2 \cdot 1$	1
-2^8	'15a7'	$C_3 \cdot C_5 = 1 \cdot 1$	2
-2^{2z} with $z \geq 5$ even		$C_2 = 2(z-4)$	
-2^{2z} with $z \geq 5$ odd		$C_2 = 2(z-4)$	

[3] This can be also shown by Tate's algorithm, applied to the equation $y^2 + \beta xy - (\beta+16)^2 y = x^3 - (\beta+96)x^2 + 192(\beta+16)x - 128(\beta+24)(\beta+16)$ for E.

So when $|\beta|$ is a power of 2, then we only need to deal with the cases $\beta = -2^{2z}$ with (i) $z = 4$ or (ii) $z \geq 3$ being odd.

4.6.2 $(\#Ш(E/K))^{1/2}$

In this subsection, we shall see $2 \mid (\#Ш(E/K))^{1/2}$, for various remaining cases left from considerations about Tamagawa numbers. Our main job is to show $\sum i_\ell + \dim \Phi \geq 4$ (notations from subsection 4.3.1). Then,

$$\boxed{\sum i_\ell + \dim \Phi \geq 4} \Longrightarrow \boxed{\dim_{\mathbf{F}_2} Ш(E/K)[2] \geq 1} \Longrightarrow \boxed{2 \mid (\#Ш(E/K))^{1/2}}.$$

The first implication follows from Kramer's theorem (see subsection 4.3.1), and the last implication is due to Kolyvagin's theorem [Kol].

From the above subsection, we only need to deal with the cases when β has at most one odd prime divisor.

Proposition 4.26. *Suppose that $|\beta|$ is a power of 2. Then by the considerations in the above subsection, it is okay to consider only when $\beta = -2^{2z}$ with*

(i) $z = 3$

(ii) $z = 4$, *or*

(iii) $z \geq 5$ *being odd.*

For these cases, we have $\dim_{\mathbf{F}_2} Ш(E/K)[2] \geq 1$, *i.e., Theorem 4.25 is true.*

Proof. (i) Suppose that $z = 3$, i.e., $\beta = -2^6$. This corresponds to the curve '24a3' having Tamagawa number $C = 2$. In this case we take the Weierstrass equation of the following form: $y^2 = x^3 + 14x^2 + x$. Note that this equation has discriminant $\Delta = 2^{10} \cdot 3$ and this is the minimal discriminant for E.

We use notations from 4.3.1. Consider the Selmer group $\mathrm{Sel}^\phi(E/\mathbf{Q})$ following [Got]. This is the subgroup of $\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$ having the following local images in $\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for each prime p (including ∞).

- $\mathrm{im}\, \delta_\infty = \{1\}$.

- $\mathrm{im}\,\delta_p = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \neq 3$.
- $\mathrm{im}\,\delta_3 = \mathbf{Q}_3^\times/\mathbf{Q}_3^{\times 2}$.
- $\mathrm{im}\,\delta_2 = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

So we have $\mathrm{Sel}^\phi(E/\mathbf{Q}) = \langle 2, 3\rangle \subset \mathbf{Q}^\times/\mathbf{Q}^{\times 2}$.

Now we consider the local norm indices. Ignoring trivial cases when $\sum i_\ell \geq 4$, and considering Heegner hypothesis, only open cases are as follows.

- $d = -q$ for an odd prime $q \equiv 3 \pmod 4$;
- $d = -qq'$ for odd primes $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$.

Suppose that $d = -q$ with $q \equiv 3 \pmod 4$, i.e., $d \equiv 1 \pmod 4$. By Heegner hypothesis, we must have $\left(\frac{-q}{3}\right) = 1$, so we have $\left(\frac{3}{q}\right) = 1$, i.e., $i_q = 2$. Moreover, in order for the prime 2 to split completely in $K = \mathbf{Q}(\sqrt{d})$, it is necessary and sufficient that $d \equiv 1 \pmod 8$, i.e., $q \equiv -1 \pmod 8$. Now we compute the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$, where E_d is the quadratic twist of E by d, and $\phi_d : E_d \longrightarrow E'_d$ is the corresponding 2-cyclic isogeny. We denote by δ_ℓ^d the corresponding homomorphism

$$E'_d(\mathbf{Q}_\ell)/\phi_d\left(E_d(\mathbf{Q}_\ell)\right) \longrightarrow H^1(\mathbf{Q}_\ell, E_d[\phi_d]).$$

Local images $\mathrm{im}\,\delta_\ell^d$ are given as follows.

- $\mathrm{im}\,\delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$,
- $\mathrm{im}\,\delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \nmid 3q$.
- $\mathrm{im}\,\delta_3^d = \mathbf{Q}_3^\times/\mathbf{Q}_3^{\times 2}$.
- $\mathrm{im}\,\delta_q^d = \{1, qu\}$ for some $u \in \mathbf{Z}_q^\times$.
- $\mathrm{im}\,\delta_2^d = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

Now, since $\left(\frac{2}{q}\right) = 1$, the image of 2 is contained in Φ and is non-trivial, whence $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$.

Suppose that $d = -qq'$ with $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$. Note also that by Heegner hypothesis, $\left(\frac{-qq'}{3}\right) = 1$ and $-qq' \equiv 1 \pmod 8$. The latter condition implies that either $q \equiv -q' \equiv 1 \pmod 8$ or $q \equiv -q' \equiv 5 \pmod 8$. It is also safe to assume $i_q = i_{q'} = 1$, whence $\left(\frac{3}{q}\right) = \left(\frac{3}{q'}\right) = -1$. Now consider the local images for the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$.

- $\mathrm{im}\,\delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$,
- $\mathrm{im}\,\delta_p^d = \mathbf{Z}_p^\times\mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \nmid 3qq'$.
- $\mathrm{im}\,\delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for odd primes $p = 3, q, q'$.
- $\mathrm{im}\,\delta_2^d = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

Hence the image of 2 is contained in Φ non-trivially, whence $\sum i_\ell + \dim_{\mathbf{F}_2}\Phi \geq 4$.

(ii) Suppose that $z = 4$, i.e., $\beta = -2^8$. This corresponds to the curve '15a7'. It has Manin constant 2. In this case we take the Weierstrass equation of the following form: $y^2 = x^3 + 62x^2 + x$. Note that this equation has discriminant $\Delta = 2^{12} \cdot 3 \cdot 5$ and E has minimal discriminant $\Delta_{\min} = 3 \cdot 5$.

As above, consider the Selmer group $\mathrm{Sel}^\phi(E/\mathbf{Q})$ following [Got].

- $\mathrm{im}\,\delta_\infty = \{1\}$.
- $\mathrm{im}\,\delta_p = \mathbf{Z}_p^\times\mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \neq 3, 5$.
- $\mathrm{im}\,\delta_p = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for odd primes $p = 3, 5$.
- $\mathrm{im}\,\delta_2 = \mathbf{Z}_2^\times\mathbf{Q}_2^{\times 2}/\mathbf{Q}_2^{\times 2}$.

So we have $\mathrm{Sel}^\phi(E/\mathbf{Q}) = \langle 3, 5\rangle$.

Now we consider the local norm indices. First note that $i_\infty = 1$. Ignoring trivial cases when $\sum i_\ell \geq 4$, and the cases violating Heegner hypothesis, we have to consider the following cases.

- $d = -q$ for an odd prime q;
- $d = -2q$ for an odd prime q;

- $d = -qq'$ for odd primes q and q'.

Suppose that $d = -q$. First assume that $q \equiv 1 \pmod 4$, i.e., $d \equiv 3 \pmod 4$. In this case the prime 2 is ramified in K, so we have nonzero i_2. As $(\Delta_{\min}, d)_{\mathbf{Q}_2} = (15, -q)_{\mathbf{Q}_2} = -1$, we have $i_2 = 1$. Then it is safe to assume $\left(\frac{15}{q}\right) = -1$, i.e., $i_q = 1$. Now consider the local images for the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$.

- $\mathrm{im}\,\delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$,
- $\mathrm{im}\,\delta_p^d = \mathbf{Z}_p^\times\mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \nmid 15q$.
- $\mathrm{im}\,\delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for odd primes $p = 3, 5$.
- $\mathrm{im}\,\delta_q^d = \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2}$.
- $\mathrm{im}\,\delta_2^d = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

Hence the image of 3 is contained in Φ non-trivially, whence $\sum i_\ell + \dim_{\mathbf{F}_2}\Phi \geq 4$.

Suppose now that $d = -q$ with $q \equiv 3 \pmod 4$, i.e., $d \equiv 1 \pmod 4$. Here the prime 2 is unramified in K, so we have $i_2 = 0$. By Heegner hypothesis, we must have $\left(\frac{-q}{5}\right) = \left(\frac{-q}{3}\right) = 1$, so we have $\left(\frac{5}{q}\right) = \left(\frac{3}{q}\right) = 1$, i.e., $\left(\frac{15}{q}\right) = 1$, i.e., $i_q = 2$. Now consider the local images for the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$.

- $\mathrm{im}\,\delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$,
- $\mathrm{im}\,\delta_p^d = \mathbf{Z}_p^\times\mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \nmid 15q$.
- $\mathrm{im}\,\delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for odd primes $p = 3, 5$.
- $\mathrm{im}\,\delta_q^d = \{1, qu\}$ for some $u \in \mathbf{Z}_q^\times$.
- $\mathrm{im}\,\delta_2^d = \mathbf{Z}_2^\times\mathbf{Q}_2^{\times 2}/\mathbf{Q}_2^{\times 2}$.

As $\left(\frac{3}{q}\right) = \left(\frac{5}{q}\right) = 1$, the image of 3 is contained in Φ non-trivially, whence $\sum i_\ell + \dim_{\mathbf{F}_2}\Phi \geq 4$.

Suppose that $d = -2q$. As $(\Delta_{\min}, d)_{\mathbf{Q}_2} = (15, -2q)_{\mathbf{Q}_2}$, for $i_2 = 2$ it is necessary and sufficient that $q \equiv -1$ or $-5 \pmod 8$, i.e., $q \equiv 3 \pmod 4$. Since $i_q \geq 1$, it is safe

to assume $q \equiv 1 \pmod 4$, i.e., $i_2 = 1$. We also assume $\left(\frac{15}{q}\right) = -1$ so that $i_q = 1$. Now consider the local images for the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$.

- $\mathrm{im}\,\delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$,
- $\mathrm{im}\,\delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \nmid 15q$.
- $\mathrm{im}\,\delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for odd primes $p = 3, 5$.
- $\mathrm{im}\,\delta_q^d = \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2}$.
- $\mathrm{im}\,\delta_2^d = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

Hence the image of 3 in Φ is nontrivial, whence $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$.

Suppose that $d = -qq'$. If the prime 2 is ramified in K, then $\sum i_\ell \geq 4$. So we assume 2 is unramified in K, i.e., $d \equiv 1 \pmod 4$. Then, without loss of generality, it is fine to assume $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$. Moreover, it is also safe to assume $i_q = i_{q'} = 1$, whence $\left(\frac{15}{q}\right) = \left(\frac{15}{q'}\right) = -1$. Now consider the local images for the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$.

- $\mathrm{im}\,\delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$,
- $\mathrm{im}\,\delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \nmid 15qq'$.
- $\mathrm{im}\,\delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for odd primes $p = 3, 5, q, q'$.
- $\mathrm{im}\,\delta_2^d = \mathbf{Z}_2^\times \mathbf{Q}_2^{\times 2}/\mathbf{Q}_2^{\times 2}$.

Hence the image of 3 is contained in Φ non-trivially, whence $\dim_{\mathbf{F}_2} \Phi \geq 1$, i.e., $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$.

(iii) Now suppose that $\beta = -2^{2z}$ with $z \geq 5$ being odd. In this case we take the Weierstrass equation of the following form: $y^2 = x^3 + \left(2^{2z-2} - 2\right) x^2 + x$. Note that this equation has discriminant $\Delta = 2^{2z}\,(2^z + 4)\,(2^z - 4) > 0$ and E has minimal discriminant $\Delta_{\min} = 2^{-12}\Delta = 2^{2z-12}\,(2^z + 4)\,(2^z - 4)$. In particular the prime 2 is always bad for E. By the consideration on the primes dividing $\beta + 16$, we assume that all of them have odd exponents. For convenience, we let $A := 2^{2z-2} - 2$. We also note that there are distinct odd primes p, p' such that $p \mid (2^z - 4)$ and $p' \mid (2^z + 4)$.

Consider the Selmer group $\mathrm{Sel}^{\phi}(E/\mathbf{Q})$ following [Got].

- $\mathrm{im}\,\delta_\infty = \{1\}$.
- $\mathrm{im}\,\delta_p = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for any odd primes $p \nmid \Delta$.
- $\mathrm{im}\,\delta_p = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for odd primes $p \mid \Delta$.
- $\mathrm{im}\,\delta_2 = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

So we have $\mathrm{Sel}^{\phi}(E/\mathbf{Q}) \cong \langle 2, p : \text{ for any odd primes } p \text{ dividing } \Delta\rangle$.

Now we consider the local norm indices. We always have $i_\infty = 1$. Ignoring trivial cases when $\sum i_\ell \geq 4$, and considering Heegner hypothesis, we have to consider the following cases.

- $d = -q$ for an odd prime $q \equiv 3 \pmod 4$;
- $d = -qq'$ for odd primes $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$.

Suppose that $d = -q$ with $q \equiv 3 \pmod 4$, i.e., $d \equiv 1 \pmod 4$. Note that $i_\infty = 1$ and $i_q \geq 1$. By Heegner hypothesis, we have $\left(\frac{-q}{p}\right) = \left(\frac{p}{q}\right) = 1$ for every odd prime p dividing Δ. Hence $\left(\frac{\Delta}{q}\right) = 1$, i.e., $i_q = 2$. Now consider the local images for the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$.

- $\mathrm{im}\,\delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$,
- $\mathrm{im}\,\delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for any odd primes $p \nmid \Delta q$.
- $\mathrm{im}\,\delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for odd primes $p \mid \Delta$.
- $\mathrm{im}\,\delta_q^d = \begin{cases} \{1, qu\} & \text{if } q \nmid A, \\ \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{otherwise.} \end{cases}$
- $\mathrm{im}\,\delta_2^d = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

Hence the image of a fixed odd prime p dividing Δ is contained in Φ non-trivially, i.e., $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$.

Suppose that $d = -qq'$ with $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$. Moreover, it is also safe to assume $i_q = i_{q'} = 1$, whence $\left(\frac{\Delta_{\min}}{q}\right) = \left(\frac{\Delta_{\min}}{q'}\right) = -1$. Now consider the local images for the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$.

- $\operatorname{im} \delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$,
- $\operatorname{im} \delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \nmid \Delta qq'$.
- $\operatorname{im} \delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for odd primes $p \mid \Delta$.
- $\operatorname{im} \delta_q^d = \begin{cases} \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{if } q \nmid A, \\ \{1, qu\} & \text{if } q \mid A, \end{cases}$ for some $u \in \mathbf{Z}_q^\times$.
- $\operatorname{im} \delta_{q'}^d = \mathbf{Q}_{q'}^\times/\mathbf{Q}_{q'}^{\times 2}$.
- $\operatorname{im} \delta_2^d = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

If there is an odd prime $p \mid \Delta$ such that $\left(\frac{p}{q}\right) = 1$, then the image of p in Φ is non-trivial, since Δ has at least 2 odd prime divisors. Suppose that $\left(\frac{p}{q}\right) = -1$ for all odd prime divisor p of Δ. In this case Δ must have ≥ 3 odd prime divisors, and thus if we pick two p and p', the image of pp' is contained in Φ and is non-trivial. In any case $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$. □

Proposition 4.27. *Suppose that $\beta = p^m$ for some $m > 0$. By the previous subsection, we assume*

- *$m = 2z$ for some positive integer z; and*
- *for all odd prime ℓ dividing $\beta + 16$, $\operatorname{ord}_\ell \Delta_{\min} = \operatorname{ord}_\ell (\beta + 16)$ is odd.*

Then we have $\dim_{\mathbf{F}_2} Ш(E/K)[2] \geq 1$, i.e., Theorem 4.25 is true, except for a family of curves defined by the equation

$$y^2 + p^z xy - p^z y = x^3 - x^2,$$

with $p^{2z} + 16 = \ell^k$ being prime powers.

Remark. For the exceptional family, Theorem 4.25 is also true. This will be shown in the following subsection 4.6.3.

Proof. We begin with the following equation: $y^2 + p^{2z}xy - p^{4z}y = x^3 - p^{2z}x^2$. By a change of variables via $[(1/2)p^z, 0, 0, 0]$, we get $y^2+2p^zxy-8p^zy = x^3-4x^2$. Making another change of variables via $[1, 4, -p^z, 0]$, we get $y^2 = x^3 + (p^{2z}+8)x^2 + 16x$. The last equation has discriminant $\Delta = 2^{12}(p^{2z}+16)p^{2z}$ and $c_4 = 16p^{4z}+256p^{2z}+256$. Note that the minimal discriminant of E is given by $\Delta_{\min} = (p^{2z}+16)p^{2z}$; in particular, E has good reduction modulo 2.

Let ϕ be the isogeny $E \longrightarrow E' := E/E(\mathbf{Q})[2]$. (Note that $E(\mathbf{Q})[2] \cong \mathbf{Z}/2\mathbf{Z}$.) Following [Got], we compute the Selmer group $\mathrm{Sel}^{\phi}(E/\mathbf{Q})$. For each prime ℓ (including ∞), we denote by δ_ℓ the map $E'(\mathbf{Q}_\ell)/\phi\left(E(\mathbf{Q}_\ell)\right) \longrightarrow H^1(\mathbf{Q}_\ell, E[\phi])$. Since $\mathrm{Sel}^{\phi}(E/\mathbf{Q}) \subset H^1(\mathbf{Q}, E[\phi]) \cong \mathbf{Q}^\times/\mathbf{Q}^{\times 2}$, the elements of $\mathrm{Sel}^{\phi}(E/\mathbf{Q})$ are those classes of $b \in \mathbf{Q}^\times$ such that their restrictions $b \in H^1(\mathbf{Q}_\ell, E[\phi]) \cong \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times 2}$ are contained in the image $\operatorname{im}\delta_\ell$. So by considering the images $\operatorname{im}\delta_\ell$, we can figure out which classes are in the Selmer group. For more details of this paragraph, see subsection 4.3.1.

These local images are given as follows.

- $\operatorname{im}\delta_\infty = \{1\}$.
- $\operatorname{im}\delta_\ell = \mathbf{Z}_\ell^\times\mathbf{Q}_\ell^{\times 2}/\mathbf{Q}_\ell^{\times 2}$ for odd primes $\ell \nmid \Delta$.
- $\operatorname{im}\delta_\ell = \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times 2}$ for odd prime $\ell \mid \Delta$, and $\ell \neq p$.
- $\operatorname{im}\delta_p = \begin{cases} \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2} & \text{if } p \equiv 1 \pmod 4, \\ \mathbf{Z}_p^\times\mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$
- $\operatorname{im}\delta_2 = \{1, 5\} \subset \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

Here are some remarks on the odd primes dividing Δ. Since $p^{2z}+16$ is a sum of two squares, so by the famous theorem on the sum of two squares, if $\ell \equiv 3 \pmod 4$ divides $\left(p^{2z}+16\right)$, then $\mathrm{ord}_\ell\left(p^{2z}+16\right)$ must be even. However, we assumed that the exponent $\mathrm{ord}_\ell\left(p^{2z}+16\right)$ is always odd. Hence any prime divisor ℓ of $\left(p^{2z}+16\right)$ must satisfy $\ell \equiv 1 \pmod 4$.

Let d be a negative, squarefree integer. We now compute the sum of local norm indices $\sum i_\ell$. Note that $i_\infty = 1$. After excluding obvious cases giving $\sum i_\ell \geq 4$, we have the following four cases:

- $d = -2$;
- $d = -q$ for an odd prime q;
- $d = -2q$ for an odd prime q;
- $d = -qq'$ for odd primes q, q'.

Suppose first that $d = -2$. As $(\Delta_{\min}, d)_{\mathbf{Q}_2} = \left((p^{2z'} + 16)p^{2z}, -2\right)_{\mathbf{Q}_2} = (1, -2)_{\mathbf{Q}_2} = 1$, we have $\sum i_\ell = 3$. Now we compute the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$, where E_d is the quadratic twist of E by d, and $\phi_d : E_d \longrightarrow E'_d$ is the corresponding 2-cyclic isogeny. We denote by δ_ℓ^d the corresponding homomorphism

$$E'_d(\mathbf{Q}_\ell)/\phi_d\left(E_d(\mathbf{Q}_\ell)\right) \longrightarrow H^1(\mathbf{Q}_\ell, E_d[\phi_d]).$$

Local images $\operatorname{im}\delta_\ell^d$ are given as follows.

- $\operatorname{im}\delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$.
- $\operatorname{im}\delta_\ell^d = \mathbf{Z}_\ell^\times\mathbf{Q}_\ell^{\times 2}/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \nmid \Delta$.
- $\operatorname{im}\delta_\ell^d = \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \mid \Delta$, with $\ell \neq p$.
- $\operatorname{im}\delta_p^d = \begin{cases} \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2} & \text{if } p \equiv \pm 1 \pmod 8, \\ \mathbf{Z}_p^\times\mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2} & \text{if } p \equiv \pm 5 \pmod 8. \end{cases}$
- $\operatorname{im}\delta_2^d = \{1, -2\}$.

By Heegner hypothesis, for any prime $\ell \mid \Delta_{\min}$, we have $\left(\frac{-2}{\ell}\right) = \left(\frac{-1}{\ell}\right)\left(\frac{2}{\ell}\right) = 1$. This implies that such an ℓ is congruent to either 1 or -5 modulo 8. However, by the sum of two squares theorem mentioned above, we must have $\ell \equiv 1 \pmod 8$ if $\ell \mid \Delta_{\min}$ and if $\ell \neq p$. If $p \equiv 1 \pmod 8$, then the image of p is contained in Φ and is non-trivial, by Proposition 4.15, and the assumptions we made in the statement

of current proposition. So suppose that $p \equiv -5 \pmod 8$. If there are two distinct odd primes ℓ and ℓ' dividing $p^{2z}+16$, then the image of ℓ or equivalently of ℓ' is contained in Φ and is non-trivial. So for these cases, we have $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$. If there is only one odd prime dividing $p^{2z}+16$, this will be covered in the following subsection 4.6.3.

Suppose that $d = -q$ for some odd prime q. Suppose first that $q \equiv 1 \pmod 4$, i.e. $d \equiv 3 \pmod 4$. As $\mathrm{disc}(\mathbf{Q}(\sqrt{d})|\mathbf{Q}) = 4d = -4q$, the prime 2 is ramified in $K = \mathbf{Q}(\sqrt{d})$. Since $(\Delta_{\min}, d)_{\mathbf{Q}_2} = (1,-q)_{\mathbf{Q}_2} = 1$ as $-q \equiv -1$ or $-5 \pmod 8$, we have $i_2 = 2$. Since $i_\infty = 1$ and $i_q \geq 1$, we always have $\sum i_\ell \geq 4$.

Now assume that $d = -q$ with a prime $q \equiv 3 \pmod 4$, then $d \equiv 1 \pmod 4$. In this case the prime 2 is unramified in K. So we have $i_2 = 0$. Let us consider the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$.

- $\mathrm{im}\,\delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$.
- $\mathrm{im}\,\delta_\ell^d = \mathbf{Z}_\ell^\times \mathbf{Q}_\ell^{\times 2}/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \nmid \Delta$, $\ell \neq q$.
- $\mathrm{im}\,\delta_\ell^d = \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \mid \Delta$, and $\ell \neq p$.
- $\mathrm{im}\,\delta_p^d = \begin{cases} \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2} & \text{if } p \equiv 1 \pmod 4, \\ \mathbf{Z}_p \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$
- $$\mathrm{im}\,\delta_q^d = \begin{cases} \{1, qu\} \subset \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{if } q \nmid \left(p^{2z}+8\right) \text{ and } \left(\dfrac{p^{2z}+16}{q}\right) = 1, \\ \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{otherwise,} \end{cases}$$
  for some $u \in \mathbf{Z}_q^\times$.
- $\mathrm{im}\,\delta_2^d = \{1, 5\}$.

Note that for any odd prime $\ell \mid \Delta$, we have $1 = \left(\dfrac{-q}{\ell}\right) = \left(\dfrac{-1}{\ell}\right)(-1)^{\frac{q-1}{2}\frac{\ell-1}{2}}\left(\dfrac{\ell}{q}\right) = \left(\dfrac{\ell}{q}\right)$. If $p \equiv 1 \pmod 4$, then the image of p is contained in Φ and is non-trivial. Even if $p \equiv 3 \pmod 4$, if there are at least two odd prime divisors of $\Delta_{\min}$ apart from p, then we also have $\dim_{\mathbf{F}_2} \Phi \geq 1$, i.e., $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$. If there is only one odd prime dividing $p^{2z}+16$, this will be covered in the following 'exceptional case' 4.6.3.

Assume $d = -2q$. We have $i_\infty = 1$ always. Note that

$$(\Delta_{\min}, d)_{\mathbf{Q}_2} = \left(p^{2z}\left(p^{2z}+16\right), -2q\right)_{\mathbf{Q}_2} = (1, -2q)_{\mathbf{Q}_2} = 1,$$

whence $i_2 = 2$. Since $i_q \geq 1$, we always have $\sum i_\ell \geq 4$.

Finally, assume $d = -qq'$. If the prime 2 is ramified in $K = \mathbf{Q}(\sqrt{d})$, then surely we have $\sum_\ell i_\ell \geq 4$. Hence, we must assume the other, i.e., 2 is unramified, which means that $d \equiv 1 \pmod 4$. Without loss of generality, we then assume $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$. Moreover, we further assume $i_q = i_{q'} = 1$, i.e., $\left(\dfrac{p^{2z}+16}{q}\right) = \left(\dfrac{p^{2z}+16}{q'}\right) = -1$. Now consider the local images of $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$ as follows.

- $\operatorname{im}\delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$.
- $\operatorname{im}\delta_\ell^d = \mathbf{Z}_\ell^\times\mathbf{Q}_\ell^{\times 2}/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \nmid \Delta$, $\ell \neq q$.
- $\operatorname{im}\delta_\ell^d = \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \mid \Delta$ and $\ell \neq p$.
- $\operatorname{im}\delta_p^d = \begin{cases} \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2} & \text{if } p \equiv 1 \pmod 4, \\ \mathbf{Z}_p\mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$
- $\operatorname{im}\delta_q^d = \begin{cases} \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{if } q \nmid \left(p^{2z}+8\right), \\ \{1, qu\} \subset \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{if } q \mid \left(p^{2z}+8\right), \end{cases}$ for some $u \in \mathbf{Z}_q^\times$.
- $\operatorname{im}\delta_{q'}^d = \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2}$.
- $\operatorname{im}\delta_2^d = \{1, 5\}$.

Note that for any odd primes ℓ dividing Δ, we get

$$1 = \left(\frac{-qq'}{\ell}\right) = \left(\frac{-1}{\ell}\right)(-1)^{\frac{\ell-1}{2}\frac{q-1}{2}}\left(\frac{\ell}{q}\right)(-1)^{\frac{\ell-1}{2}\frac{q'-1}{2}}\left(\frac{\ell}{q'}\right) = \left(\frac{\ell}{q}\right)\left(\frac{\ell}{q'}\right)$$

and thus we have either $\left(\dfrac{\ell}{q}\right) = \left(\dfrac{\ell}{q'}\right) = 1$ or $\left(\dfrac{\ell}{q}\right) = \left(\dfrac{\ell}{q'}\right) = -1$. Suppose first that $p \equiv 1 \pmod 4$. If $\left(\dfrac{p}{q}\right) = 1$, then we are done, since the image of p in Φ is non-trivial.

If $\left(\frac{p}{q}\right) = -1$, then the image of either p or pq in Φ is non-trivial. Now, suppose that $p \equiv 3 \pmod 4$. If there are at least two distinct prime divisors of $p^{2z} + 16$, then among those divisors, at least one ℓ must have $\left(\frac{\ell}{q}\right) = 1$, since $\left(\frac{p^{2z}+16}{q}\right) = -1$. For these cases we have $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$. If there is only one odd prime dividing $p^{2z} + 16$, this will be covered in the following 'exceptional case' 4.6.3.

So far, we have shown that for any cases of d, we obtain $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$ with a family of exceptions. Thus by Kramer's formula, we have $4 \mid C \cdot (\#Ш(E/K))^{1/2}$ for the curves not in the exceptional family. □

Proposition 4.28. *Suppose that $\beta = -p^m$ for some $m > 0$. By the previous subsection, we assume $m = 2z$ for some positive integer z. Then we have* $\dim_{\mathbf{F}_2} Ш(E/K)[2] \geq 1$, *i.e., Theorem 4.25 is true.*

Proof. We begin with the equation (4.14): $y^2 - p^{2z}xy - p^{4z}y = x^3 + p^{2z}x^2$. By a change of variables via $[(1/2)p^z, 0, 0, 0]$, we get $y^2 - 2p^z xy - 8p^z y = x^3 + 4x^2$. Making another change of variables via $[1, -4, p^z, 0]$, we get $y^2 = x^3 + (p^{2z} - 8)x^2 + 16x$. The last equation has discriminant $\Delta = 2^{12}(p^{2z} - 16)p^{2z}$ and $c_4 = 16p^{4z} - 256p^{2z} + 256$. Since $\Delta < 0$ if and only if $p = 3$ and $z = 1$, and in this case E is the curve '21a4', having Tamagawa number 2 and Manin constant 2. So in the sequel, we assume $\Delta > 0$ always. Note that the minimal discriminant of E is given by $\Delta_{\min} = (p^{2z} - 16)p^{2z}$; in particular, E has good reduction modulo 2.

Following [Got], we compute the Selmer group $\mathrm{Sel}^{\phi}(E/\mathbf{Q})$.

- $\operatorname{im} \delta_\infty = \{1\}$.
- $\operatorname{im} \delta_\ell = \mathbf{Z}_\ell^\times \mathbf{Q}_\ell^{\times 2}/\mathbf{Q}_\ell^{\times 2}$ for odd primes $\ell \nmid \Delta$.
- $\operatorname{im} \delta_\ell = \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times 2}$ for odd prime $\ell \mid \Delta$ including p.
- $\operatorname{im} \delta_2 = \{1, 5\} \subset \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

Here are some remarks on the odd primes dividing Δ. As $\Delta = 2^{12}p^{2z}\left(p^{2z} - 16\right) = 2^{12}p^{2z}\left(p^z - 4\right)\left(p^z + 4\right)$, if $\left(p^z - 4\right) \neq \pm 1$, there are at least two odd primes other than p dividing Δ. If $\left(p^z - 4\right) = 1$, then we have $p = 5$ and $z = 1$, which yield the

curve '15a3', having $C_3 = C_5 = 2$. Similarly, if $(p^z - 4) = -1$, then E is the curve '21a4' having $C_3 = 2$, $C_7 = 1$, and $M = 2$. So we exclude these curves from our consideration and assume that there are two distinct odd primes p', p'' such that $p' \mid (p^z - 4)$ and $p'' \mid (p^z + 4)$.

Let d be a negative, square-free integer. We now compute the sum of local norm indices $\sum i_\ell$. Note that $i_\infty = 1$. After excluding obvious cases giving $\sum i_\ell \geq 4$, we have the following four cases:

- $d = -2$;
- $d = -q$ for an odd prime q;
- $d = -2q$ for an odd prime q;
- $d = -qq'$ for odd primes q, q'.

Suppose first that $d = -2$. As $(\Delta_{\min}, d)_{\mathbf{Q}_2} = \left((p^{2z} - 16)p^{2z}, -2\right)_{\mathbf{Q}_2} = (1, -2)_{\mathbf{Q}_2} = 1$, we have $\sum i_\ell = 3$. Now we compute the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$. Local images are given as follows.

- $\mathrm{im}\, \delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$.
- $\mathrm{im}\, \delta_\ell^d = \mathbf{Z}_\ell^\times \mathbf{Q}_\ell^{\times 2}/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \nmid \Delta$.
- $\mathrm{im}\, \delta_\ell^d = \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \mid \Delta$, including $\ell = p$.
- $\mathrm{im}\, \delta_2^d = \{1, -2\}$.

If $p \equiv 1 \pmod 4$, then since $1 = \left(\dfrac{-2}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}$, we have $p \equiv 1 \pmod 8$. So the image of p is contained in Φ and is non-trivial. Suppose that $p \equiv 3 \pmod 4$, this means that $p \equiv -5 \pmod 8$. Now, for any prime ℓ dividing $p^{2z} - 16$, we have $1 = \left(\dfrac{-2}{\ell}\right)$, so that we have either $\ell \equiv 1 \pmod 8$ or $\ell \equiv -5 \pmod 8$. In any case, since there are at least two prime divisors in $p^{2z} - 16$, either the image of ℓ or ℓp must be congruent to 1 modulo 8, and thus the image is contained in Φ non-trivially. Thus we have $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$.

Suppose that $d = -q$ for some odd prime q. Suppose first that $q \equiv 1 \pmod 4$, i.e. $d \equiv 3 \pmod 4$. As $\mathrm{disc}(\mathbf{Q}(\sqrt{d})|\mathbf{Q}) = 4d = -4q$, the prime 2 is ramified in $K = \mathbf{Q}(\sqrt{d})$. Since $(\Delta_{\min}, d)_{\mathbf{Q}_2} = (1, -q)_{\mathbf{Q}_2} = 1$, we have $i_2 = 2$. Since $i_\infty = 1$ and $i_q \geq 1$, we always have $\sum i_\ell \geq 4$.

Now assume that $d = -q$ with a prime $q \equiv 3 \pmod 4$, then $d \equiv 1 \pmod 4$. In this case the prime 2 is unramified in K. So we have $i_2 = 0$. Let us consider the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$.

- $\mathrm{im}\,\delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$.
- $\mathrm{im}\,\delta_\ell^d = \mathbf{Z}_\ell^\times \mathbf{Q}_\ell^{\times 2}/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \nmid \Delta$, $\ell \neq q$.
- $\mathrm{im}\,\delta_\ell^d = \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \mid \Delta$, including $\ell = p$.
- $\mathrm{im}\,\delta_q^d = \begin{cases} \{1, qu\} \subset \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{if } q \nmid \left(p^{2z} - 8\right) \text{ and } \left(\dfrac{p^{2z} - 16}{q}\right) = 1, \\ \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{otherwise,} \end{cases}$ for some $u \in \mathbf{Z}_q^\times$.
- $\mathrm{im}\,\delta_2^d = \{1, 5\}$.

Note that for any odd prime $\ell \mid \Delta$, we have $1 = \left(\dfrac{-q}{\ell}\right) = \left(\dfrac{-1}{\ell}\right)(-1)^{\frac{q-1}{2}\frac{\ell-1}{2}}\left(\dfrac{\ell}{q}\right) = \left(\dfrac{\ell}{q}\right)$. So if $p \equiv 1 \pmod 4$, then the image of p is contained in Φ and is non-trivial. Suppose $p \equiv 3 \pmod 4$. If there is a prime ℓ dividing $p^{2z} - 16$ such that $\ell \equiv 1 \pmod 4$, then the image of ℓ in Φ is non-trivial, since there are at least two odd prime divisors dividing $p^{2z} - 16$. If $\ell \equiv 3 \pmod 4$, then the image of ℓp will do the same job. Thus we have $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$.

Assume $d = -2q$. We have $i_\infty = 1$ always. Note that

$$(\Delta_{\min}, d)_{\mathbf{Q}_2} = \left(p^{2z}\left(p^{2z} - 16\right), -2q\right)_{\mathbf{Q}_2} = (1, -2q)_{\mathbf{Q}_2} = 1,$$

whence $i_2 = 2$. Since $i_q \geq 1$, we always have $\sum i_\ell \geq 4$.

Finally, assume $d = -qq'$. If the prime 2 is ramified in $K = \mathbf{Q}(\sqrt{d})$, then surely we have $\sum_\ell i_\ell \geq 4$. Hence, we must assume the other, i.e., 2 is unramified, which means that $d \equiv 1 \pmod 4$. Without loss of generality, we then assume $q \equiv 1 \pmod 4$

and $q' \equiv 3 \pmod 4$. Moreover, we further assume $i_q = i_{q'} = 1$, i.e., $\left(\frac{p^{2z}-16}{q}\right) = \left(\frac{p^{2z}-16}{q'}\right) = -1$. Now consider the local images of $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$ as follows.

- $\mathrm{im}\,\delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$.
- $\mathrm{im}\,\delta_\ell^d = \mathbf{Z}_\ell^\times\mathbf{Q}_\ell^{\times 2}/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \nmid \Delta$, $\ell \neq q$.
- $\mathrm{im}\,\delta_\ell^d = \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \mid \Delta$ including $\ell = p$.
- $\mathrm{im}\,\delta_q^d = \begin{cases} \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{if } q \nmid \left(p^{2z}-8\right), \\ \{1, qu\} \subset \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{if } q \mid \left(p^{2z}-8\right), \end{cases}$ for some $u \in \mathbf{Z}_q^\times$.
- $\mathrm{im}\,\delta_{q'}^d = \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2}$.
- $\mathrm{im}\,\delta_2^d = \{1, 5\}$.

Note that for any odd primes ℓ dividing Δ, we get

$$1 = \left(\frac{-qq'}{\ell}\right) = \left(\frac{-1}{\ell}\right)(-1)^{\frac{\ell-1}{2}\frac{q-1}{2}}\left(\frac{\ell}{q}\right)(-1)^{\frac{\ell-1}{2}\frac{q'-1}{2}}\left(\frac{\ell}{q'}\right) = \left(\frac{\ell}{q}\right)\left(\frac{\ell}{q'}\right)$$

and thus we have either $\left(\frac{\ell}{q}\right) = \left(\frac{\ell}{q'}\right) = 1$ or $\left(\frac{\ell}{q}\right) = \left(\frac{\ell}{q'}\right) = -1$. Suppose first that $p \equiv 1 \pmod 4$. If $\left(\frac{p}{q}\right) = 1$, then we are done, since the image of p in Φ is non-trivial. So suppose that $\left(\frac{p}{q}\right) = -1$. In this case we consider the prime divisors of $p^{2z} - 16$. If there is a prime divisor $\ell \mid \left(p^{2z} - 16\right)$ such that $\ell \equiv 1 \pmod 4$, then the image of either p or ℓp is contained in Φ non-trivially. So suppose that all the prime divisors of $p^{2z} - 16$ are congruent to 3 modulo 4. Since $\left(\frac{p^{2z}-16}{q}\right) = -1$, we can find a prime divisor ℓ of $p^{2z} - 16$ satisfying $\left(\frac{\ell}{q}\right) = -1$. We suppose that such ℓ is unique, for if there is another one, then its product with ℓ has non-trivial image in Φ, because there should be the third one since $\left(\frac{p^{2z}-16}{q}\right) = -1$. If there are two distinct prime

divisors ℓ' and ℓ'' such that $\ell' \equiv \ell'' \equiv 3 \pmod 4$ and $\left(\frac{\ell'}{q}\right) = \left(\frac{\ell''}{q}\right) = 1$, then the image of $\ell'\ell''$ in Φ is non-trivial, because of the existence of ℓ. So the only remaining case is when $p^{2z} - 16$ has only two prime divisors ℓ and ℓ' with $\ell \equiv \ell' \equiv 3 \pmod 4$, $\left(\frac{\ell}{q}\right) = -1$ and $\left(\frac{\ell'}{q}\right) = 1$. However, we can factor $p^{2z} - 16 = (p^z - 4)(p^z + 4)$ and since $p \equiv 1 \pmod 4$, we must have either $p^z - 4 = 1$ or $p^z + 4 = 1$, which we excluded in our consideration above.

Suppose that $p \equiv 3 \pmod 4$ and $\left(\frac{p}{q}\right) = 1$. If there is a prime $\ell \mid \left(p^{2z} - 16\right)$ with $\left(\frac{\ell}{q}\right) = 1$, then the image of ℓ or ℓp in Φ is non-trivial. Hence, we can assume that every prime divisor ℓ of $p^{2z} - 16$ must satisfy $\left(\frac{\ell}{q}\right) = -1$. Since $\left(\frac{p^{2z} - 16}{q}\right) = -1$, then we conclude that the number of prime divisors of $p^{2z} - 16$ is odd, and $\neq 1$ because we exclude the cases when $p^{2z} - 16$ is a prime power. Then, in any cases, we always find two primes ℓ' and ℓ'' such that $\ell' \equiv \ell'' \pmod 4$. By considering the image of $\ell'\ell''$ in Φ we can obtain the desired result. Now, let us assume that $p \equiv 3 \pmod 4$ and $\left(\frac{p}{q}\right) = -1$. Similar arguments show that we must have $\dim_{\mathbf{F}_2} \Phi \geq 1$.

So far, we have shown that for any cases of d, we obtain $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$. Thus by Kramer's formula, we have $4 \mid C \cdot (\#Ш(E/K))^{1/2}$. □

Proposition 4.29. *Suppose that $\beta = \pm 2^m p^{m'}$ for some $m, m' > 0$. By the considerations of the above subsection, we assume*

- *$m' = 2z$ for some $z \in \mathbf{Z}_{>0}$, and*
- *$m = 8$ and $u = \pm p^{m'} \equiv 3 \pmod 4$,*

i.e., $\beta = -2^8 p^{2z}$ for some odd z. Then we have $\dim_{\mathbf{F}_2} Ш(E/K)[2] \geq 1$, i.e., Theorem 4.25 is true.

Proof. The Weierstrass equation then becomes: $y^2 - 2^8 p^{2z} xy - 2^{16} p^{4z} y = x^3 + 2^8 p^{2z} x^2$. We first make a change of variables via $[p^z 2^4, 0, 0, 0]$ to obtain: $y^2 - 16p^z xy - 16p^z y = x^3 + x^2$, and again via $[1, -1, 8p^z, 0]$, we get

$$y^2 = x^3 + \left(64p^{2z} - 2\right) x^2 + x. \tag{4.15}$$

The final equation has $\Delta = 2^{12}p^{2z}\,(4p^z+1)\,(4p^z-1)$ and $c_4 = 65536p^{4z} - 4096p^{2z} + 16$. Note that the minimal discriminant of E is $\Delta_{\min} = p^{2z}\,(4p^z+1)\,(4p^z-1)$. Since E has reduction of type $\mathrm{I}_{\mathrm{ord}_\ell \Delta_{\min}}$ modulo a prime $\ell \neq p$ dividing $\Delta_{\min}$, we assume $\mathrm{ord}_\ell \Delta_{\min}$ is odd.

Following [Got], we compute the Selmer group $\mathrm{Sel}^\phi(E/\mathbf{Q}) = \bigcap_\ell \mathrm{im}\,\delta_\ell$ inside of $\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$. Local images are given as follows.

- $\mathrm{im}\,\delta_\infty = \{1\}$.
- $\mathrm{im}\,\delta_\ell = \mathbf{Z}_\ell^\times \mathbf{Q}_\ell^{\times 2}/\mathbf{Q}_\ell^{\times 2}$ for odd primes $\ell \nmid \Delta$.
- $\mathrm{im}\,\delta_\ell = \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times 2}$ for odd prime $\ell \mid \Delta$ including $\ell = p$.
- $\mathrm{im}\,\delta_2 = \mathbf{Z}_2^\times \mathbf{Q}_2^{\times 2}/\mathbf{Q}_2^{\times 2}$.

Here is a remark on the odd primes dividing Δ. As

$$\Delta = 2^{12}p^{2z}\,(4p^z+1)\,(4p^z-1)\,,$$

there are at least one odd prime not equal to p dividing each $(4p^z+1)$ and $(4p^z-1)$. Note also that we cannot have an odd prime dividing both $(4p^z+1)$ and $(4p^z-1)$, for if so, then the prime would also divide $(4p^z+1)-(4p^z-1) = 2$, a contradiction. Hence there are at least three odd primes dividing Δ, i.e., p, one dividing $(4p^z+1)$, and another dividing $(4p^z-1)$.

Let d be a negative, squarefree integer such that $K = \mathbf{Q}(\sqrt{d})$. We now compute the sum of local norm indices $\sum i_\ell$. Note that $i_\infty = 1$. After excluding obvious cases giving $\sum i_\ell \geq 4$, it remains the following four cases: $d = -2$; $d = -q$ for an odd prime q; $d = -2q$ for an odd prime q; and $d = -qq'$ for odd primes q, q'.

Suppose first that $d = -2$. As

$$(\Delta_{\min}, d)_{\mathbf{Q}_2} = \left(p^{2z}\left(16p^{2z}-1\right), -2\right)_{\mathbf{Q}_2} = (-1,-2)_{\mathbf{Q}_2} = -1,$$

we have $\sum i_\ell = 2$. Now we compute the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q}) = \bigcap_\ell \mathrm{im}\,\delta_\ell \subset \mathbf{Q}^\times/\mathbf{Q}^{\times 2}$. Local images are given as follows.

- $\mathrm{im}\,\delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$.

- $\operatorname{im} \delta_\ell^d = \mathbf{Z}_\ell^\times \mathbf{Q}_\ell^{\times 2}/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \nmid \Delta$.
- $\operatorname{im} \delta_\ell^d = \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \mid \Delta$ (including $\ell = p$).
- $\operatorname{im} \delta_2^d = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

As the images of p and the images of a prime dividing, say, $(4p^z + 1)$ must go to distinct non-trivial element in $H^1(\mathbf{Q}, E[2])$ and in $H^1(\mathbf{Q}, E_d[2])$, they define distinct elements in the Selmer group $\mathrm{Sel}^2(E/\mathbf{Q})$ and $\mathrm{Sel}^2(E_d/\mathbf{Q})$. Thus there are at least two non-trivial elements in Φ, whence $\dim_{\mathbf{F}_2} \Phi \geq 2$. Hence $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$.

Suppose that $d = -q$ for some odd prime q. Suppose first that $q \equiv 1 \pmod 4$, i.e. $d \equiv 3 \pmod 4$. As $\mathrm{disc}(\mathbf{Q}(\sqrt{d})|\mathbf{Q}) = 4d = -4q$, the prime 2 is ramified in $K = \mathbf{Q}(\sqrt{d})$. Since $(\Delta_{\min}, d)_{\mathbf{Q}_2} = (-1, -q)_{\mathbf{Q}_2} = -1$ as $-q \equiv -1$ or $-5 \pmod 8$, we have $i_2 = 1$. Thus, without loss of generality we assume $i_q = 1$ also. This is equivalent to the condition that the right hand side of the Weierstrass equation (4.15) does *not* split completely in $\mathbf{F}_q$. Thus we assume $\left(\dfrac{\left(64p^{2z} - 2\right)^2 - 4}{q}\right) = \left(\dfrac{2^8 p^{2z}\left(16p^{2z} - 1\right)}{q}\right) = \left(\dfrac{16p^{2z} - 1}{q}\right) = -1$. Taking the sum, we have $\sum i_\ell = 3$. Now let us compute the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$.

- $\operatorname{im} \delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$.
- $\operatorname{im} \delta_\ell^d = \mathbf{Z}_\ell^\times \mathbf{Q}_\ell^{\times 2}/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \nmid \Delta$, $\ell \neq q$.
- $\operatorname{im} \delta_\ell^d = \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \mid \Delta$ including $\ell = p$.
- $\operatorname{im} \delta_q^d = \begin{cases} \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{if } q \nmid \left(64p^{2z} - 2\right), \\ \{1, qu\} \subset \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{if } q \mid \left(64p^{2z} - 2\right), \end{cases}$ for some $u \in \mathbf{Z}_q^\times$.
- $\operatorname{im} \delta_2^d = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

Suppose that $q \nmid \left(64p^{2z} - 2\right)$. In this case distinct odd primes ℓ dividing Δ must define distinct elements in Φ, whence $\dim_{\mathbf{F}_2} \Phi \geq 1$, i.e., $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$. Suppose then $q \mid \left(64p^{2z} - 2\right)$. In this case as an element of $\mathrm{Sel}^{\phi_d}(E/\mathbf{Q})$, only those contained

in the local image $\{1, qu\} \subset \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2}$ are allowed. If ℓ is an odd prime dividing Δ, then by Heegner hypothesis, $1 = \left(\frac{-q}{\ell}\right) = \left(\frac{-1}{\ell}\right)\left(\frac{\ell}{q}\right)$. So if there is an odd prime $\ell \equiv 1 \pmod 4$, with $\ell \mid \Delta$, then the image of ℓ is contained in Φ, since there are at least two primes dividing $(4p^z+1)\,(4p^z-1)$, and the image of ℓ cannot be trivial. If all odd primes $\ell \mid \Delta$ are congruent to -1 modulo 4, then by choosing a prime $\ell \mid (4p^z+1)\,(4p^z-1)$, the image of ℓp is contained in Φ, and is non-trivial. In any cases, we have $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$.

Now assume that $d = -q$ with a prime $q \equiv 3 \pmod 4$, then $d \equiv 1 \pmod 4$. In this case the prime 2 is unramified in K. So we have $i_2 = 0$. Let us consider the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$.

- $\operatorname{im}\delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$.
- $\operatorname{im}\delta_\ell^d = \mathbf{Z}_\ell^\times\mathbf{Q}_\ell^{\times 2}/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \nmid \Delta$, $\ell \neq q$.
- $\operatorname{im}\delta_\ell^d = \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \mid \Delta$ (including $\ell = p$).
- $\operatorname{im}\delta_q^d = \begin{cases} \{1, qu\} \subset \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{if } q \nmid \left(64p^{2z}-2\right) \text{ and } \left(\frac{16p^{2z}-1}{q}\right) = 1, \\ \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{otherwise,} \end{cases}$ for a $u \in \mathbf{Z}_q^\times$.
- $\operatorname{im}\delta_2^d = \mathbf{Z}_2^\times\mathbf{Q}_2^{\times 2}/\mathbf{Q}_2^{\times 2}$.

Note that for any odd prime $\ell \mid \Delta$, we have $1 = \left(\frac{-q}{\ell}\right) = \left(\frac{-1}{\ell}\right)(-1)^{\frac{q-1}{2}\frac{\ell-1}{2}}\left(\frac{\ell}{q}\right) = \left(\frac{\ell}{q}\right)$. Thus the image of any odd prime $\ell \mid \Delta$ is contained in Φ, and is not trivial since there are at least 3 odd primes dividing Δ, we have $\dim_{\mathbf{F}_2}\Phi \geq 2$, regardless of the local image $\operatorname{im}\delta_q$ above. Therefore $\sum i_\ell + \dim_{\mathbf{F}_2}\Phi \geq 4$.

Assume $d = -2q$. We have $i_\infty = 1$ always. Since $i_2 \geq 1$ and $i_q \geq 1$, we have $\sum i_\ell \geq 4$ except when $i_2 = 1$ and $i_q = 1$. Since $i_2 = 1$ if and only if $(\Delta_{\min}, d)_{\mathbf{Q}_2} = \left(p^{2z}\left(16p^{2z}-1\right), -2q\right)_{\mathbf{Q}_2} = (-1,-2q)_{\mathbf{Q}_2} = -1$, we assume $q \equiv 1$ or $5 \pmod 8$. In order to have $i_q = 1$, we also assume $\left(\frac{\left(64p^{2z}-2\right)^2-4}{q}\right) = \left(\frac{2^8p^{2z}\left(16p^{2z}-1\right)}{q}\right) =$

$\left(\frac{16p^{2z}-1}{q}\right) = -1$. Now consider the local images of $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$ as follows.

- $\mathrm{im}\,\delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$.
- $\mathrm{im}\,\delta_\ell^d = \mathbf{Z}_\ell^\times\mathbf{Q}_\ell^{\times 2}/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \nmid \Delta$, $\ell \neq q$.
- $\mathrm{im}\,\delta_\ell^d = \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \mid \Delta$ (including $\ell = p$).
- $\mathrm{im}\,\delta_q^d = \begin{cases} \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{if } q \nmid \left(64p^{2z}-2\right), \\ \{1, qu\} \subset \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{if } q \mid \left(64p^{2z}-2\right), \end{cases}$ for some $u \in \mathbf{Z}_q^\times$.
- $\mathrm{im}\,\delta_2^d = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

So if there is an odd prime $\ell \mid \Delta$ such that $\left(\frac{\ell}{q}\right) = 1$ then the image of ℓ is contained in Φ, since there are at least two primes dividing $(4p^z+1)\,(4p^z-1)$, the image of ℓ cannot be trivial. If all odd primes $\ell \mid \Delta$ satisfy $\left(\frac{\ell}{q}\right) = -1$, then by choosing a prime $\ell \mid (4p^z+1)\,(4p^z-1)$, the image of ℓp is contained in Φ and is non-trivial. In any cases, we have $\sum i_\ell + \dim_{\mathbf{F}_2}\Phi \geq 4$.

Finally, assume $d = -qq'$. If the prime 2 is ramified in $K = \mathbf{Q}(\sqrt{d})$, then surely we have $\sum_\ell i_\ell \geq 4$. Hence, we must assume the other, i.e., 2 is unramified, which means that $d \equiv 1 \pmod 4$. Without loss of generality, we then assume $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$. Moreover, we further assume $i_q = i_{q'} = 1$, i.e., $\left(\frac{16p^{2z}-1}{q}\right) = \left(\frac{16p^{2z}-1}{q'}\right) = -1$. Now consider the local images of $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$ as follows.

- $\mathrm{im}\,\delta_\infty^d = \mathbf{R}^\times/\mathbf{R}^{\times 2}$.
- $\mathrm{im}\,\delta_\ell^d = \mathbf{Z}_\ell^\times\mathbf{Q}_\ell^{\times 2}/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \nmid \Delta$, $\ell \neq q$.
- $\mathrm{im}\,\delta_\ell^d = \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times 2}$ for any odd prime $\ell \mid \Delta$ (including $\ell = p$).
- $\mathrm{im}\,\delta_q^d = \begin{cases} \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{if } q \nmid \left(64p^{2z}-2\right), \\ \{1, qu\} \subset \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{if } q \mid \left(64p^{2z}-2\right), \end{cases}$ for some $u \in \mathbf{Z}_q^\times$.
- $\mathrm{im}\,\delta_{q'}^d = \mathbf{Q}_{q'}^\times/\mathbf{Q}_{q'}^{\times 2}$.

- $\operatorname{im} \delta_2^d = \mathbf{Z}_2^\times \mathbf{Q}_2^{\times 2}/\mathbf{Q}_2^{\times 2}$.

If $q \nmid \left(64p^{2z} - 2\right)$ then we are done as above. Suppose that $q \mid \left(64p^{2z} - 2\right)$. By Heegner hypothesis, we have $1 = \left(\frac{-qq'}{\ell}\right) = \left(\frac{\ell}{q}\right)\left(\frac{\ell}{q'}\right)$ for all odd primes $\ell \mid \Delta$. Hence, we may assume that $\left(\frac{\ell}{q}\right) = \left(\frac{\ell}{q'}\right) = -1$ for all such ℓ. In this case the image of ℓp in Φ is non-trivial, whence $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$.

So far, we have shown that for any cases of d, we obtain $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$. Thus by Kramer's formula, we have $4 \mid C \cdot (\#Ш(E/K))^{1/2}$. □

4.6.3 Exceptional case

This family is parametrised by the following Weierstrass equation:

$$E : y^2 + p^z xy - p^z y = x^3 - x^2,$$

where p is an odd prime congruent to 3 modulo 4. We consider the cases when $p^{2z} + 16$ is an odd power of a prime, in other words, $p^{2z} + 16 = q^k$ for some odd prime q and odd integer k. When $k > 1$, such Diophantine equation has only integer solution $p^z = 3$, $q = 5$, and $k = 2$, c.f. [CCS], Lemma 5.5. But this case corresponds to the curve '15a3', having torsion subgroup $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$. So we can exclude it from our consideration, and we may assume $k = 1$, i.e., $p^{2z} + 16$ is a prime.

Here the discriminant $\Delta = p^{2z}\left(p^{2z} + 16\right) = p^{2z}q$, which is the minimal discriminant. The conductor of the curve E is pq, and $E(\mathbf{Q})_{\text{tors}} = \mathbf{Z}/4\mathbf{Z}$.

Let G be the unique subgroup of $E(\mathbf{Q})_{\text{tors}}$ of order 2, and let E' be the curve E/G. We can find a Weierstrass equation for E' thanks to Vélu's formulae (cf. [MMR]). The Weierstrass equation for E' is given as follows:

$$y^2 + p^z xy - p^z y = x^3 - x^2 - 5x - (p^{2z} + 3),$$

with discriminant $\Delta' = p^{4z}(p^{2z} + 16)^2$. Factoring 2-torsion polynomial, we see that E' contains the full 2-torsion subgroup in $E'(\mathbf{Q})$: their x-coordinates are: 3, -1, and $-\left(p^{2z} + 1\right)/4$. In particular, the weak Gross–Zagier conjecture is true for E' (cf. §4.4 and §4.5). Now the next corollary follows from the isogeny invariance of the Gross–Zagier conjecture.

Corollary 4.30 (to Proposition 4.16)**.** *The weak Gross–Zagier conjecture is true for the elliptic curve E in the family and the quadratic field K satisfying Heegner hypothesis.*

Proof. Take $\theta : E' \longrightarrow E$ be the isogeny dual to $E \longrightarrow E/G$ and take modular parametrisations respecting θ, i.e., we first choose a modular parametrisation π' of E' and let $\pi = \theta \circ \pi'$ be the modular parametrisation for E. By Proposition 4.16 (c), and by the remark just below the proposition, for a fixed E in the family, the weak Gross–Zagier conjecture is true except possibly for at most 4 quadratic fields. Since we only concern 2-divisibility, let us try to figure out the quadratic fields satisfying $2 = \mathrm{ord}_2 E'(\mathbf{Q})_{\mathrm{tors}} < \mathrm{ord}_2 E'(K)_{\mathrm{tors}}$. If this inequality is satisfied, then $E'(K)_{\mathrm{tors}}$ must contain a point of exact order 4.

The 4-torsion polynomial for E' (i.e., the polynomial whose roots are the x-coordinates of the points in $E'[4](\overline{\mathbf{Q}})$) is given as follows:

$$f_1(x) f_2(x) f_3(x) g(x)$$

where

- $f_1(x) = 2x^2 + (p^{2z} + 4)x + (-p^{2z} + 2)$,
- $f_2(x) = x^2 - 6x - (p^{2z} + 7)$,
- $f_3(x) = x^2 + 2x + (p^{2z} + 1)$,
- $g(x) = \left(4x + p^{2z} + 4\right)(x + 1)(x - 3)$.

Evidently, the roots of $g(x)$ correspond to points in $E'[2]$. Discriminants d_i of $f_i(x)$ are as follows:

- $d_1 = p^{2z}\left(p^{2z} + 16\right) = p^{2z} q$,
- $d_2 = 4\left(p^{2z} + 16\right) = 4q$,
- $d_3 = -4p^{2z}$.

Thus if $K = \mathbf{Q}(\sqrt{d})$ is a quadratic field, the polynomials $f_i(x)$ do not have roots in K unless $K = \mathbf{Q}(\sqrt{-1})$ or $K = \mathbf{Q}(\sqrt{q})$. Note that $\mathbf{Q}(\sqrt{q})$ is a real quadratic field, which is not in our concern. If $K = \mathbf{Q}(\sqrt{-1})$, then we have $u_K = 2$. As we already knew $2 \mid C_E \cdot (\#Ш(E/K))^{1/2}$, we have $4 \mid u_K \cdot C_E \cdot (\#Ш(E/K))^{1/2}$, and the weak Gross–Zagier conjecture is also true for this case. □

4.7 $E(\mathbf{Q})_{\mathrm{tors}} \cong \mathbf{Z}/2\mathbf{Z}$

Theorem 4.31. *If E is an elliptic curve defined over $\mathbf{Q}$, having rational torsion subgroup $E(\mathbf{Q})_{\mathrm{tors}}$ isomorphic to $\mathbf{Z}/2\mathbf{Z}$, then the order $2 = \#E(\mathbf{Q})_{\mathrm{tors}}$ divides $u_K \cdot C \cdot M \cdot (\#Ш(E/K))^{1/2}$.*

For such elliptic curves, we can find a Weierstrass model following Kubert [Kub]:

$$y^2 = x^3 + Ax^2 + Bx, \tag{4.16}$$

where $A, B \in \mathbf{Z}$. Note that A and B are not necessarily relatively prime. This elliptic curve has discriminant $\Delta = 16B^2(A^2 - 4B)$ and $c_4 = 16(A^2 - 3B)$. Let N be the conductor of E, and $\Delta_{\min}$ be the minimal discriminant of E.

4.7.1 Tamagawa numbers

The purpose of this subsection is to compute Tamagawa numbers of E at various primes, in order to reduce the cases. Remaining cases will be dealt with in the subsequent subsections. More precisely, we show the following.

Proposition 4.32. *Let E be an elliptic curve defined by the equation* (4.16).

(i) If $\gcd(A, B) \neq 1$, *i.e., if there is a common prime dividing both A and B, then* $2 \mid C$.

(ii) If $B \notin \{1, -1, 16, -16\}$, *then* $2 \mid C$.

(iii) If p is an odd prime such that $\mathrm{ord}_p\left(A^2 - 4B\right)$ *is even, then* $2 \mid C_p$.

Proof. (a) Let p be a prime dividing both A and B. First of all, if both $\mathrm{ord}_p A \geq 2$ and $\mathrm{ord}_p B \geq 4$ are true, then we can make a change of variables via $[p, 0, 0, 0]$ to get another equation of the same form as equation (4.16) with (A, B) replaced by $(A/p^2, B/p^4)$. Consequently, we assume either $\mathrm{ord}_p A < 2$ or $\mathrm{ord}_p B < 4$. Using Tate's algorithm, we find reduction types for E modulo p as summarised in the following.

$\operatorname{ord}_p B$	$\operatorname{ord}_p A$	$E \bmod p$	C_p
1		III	2
2		I_k^* for some k	even
3	1	I_k^* for some k	even
	≥ 2	III^*	2
≥ 4	1 (bindingly)	I_k^* for some k	even

(b) Let p be a prime such that $p \mid B$ but $p \nmid A$. Using Tate's algorithm, we have the following results.

	$\operatorname{ord}_p B$	$A \mod 4$	$E \bmod p$	C_p
$p \neq 2$			I_n with $n = \operatorname{ord}_p \Delta = 2 \operatorname{ord}_p B$	even
$p = 2$	1		III	2
	2		I_k for some k	even
	≥ 3	-1	I_k for some k	even
	3	1	III^*	even
	4		I_0 (good)	1
	≥ 5		I_n with $n = \operatorname{ord}_p \Delta = 2 \operatorname{ord}_p B - 8$	even

In particular, if $B \notin \{1, -1, 16, -16\}$, we always have $2 \mid C$.

(c) Let p be an odd prime such that $\operatorname{ord}_p \left(A^2 - 4B\right)$ is an even positive integer. By (a), we assume $p \nmid AB$. Tate's algorithm tells us that in this case, E has reduction of type $\mathrm{I}_{\operatorname{ord}_p (A^2 - 4B)}$, and we have $2 \mid C_p$. □

Proposition 4.33. *Let E be an elliptic curve defined by the equation* (4.16).

(i) Suppose that $B = 1$. If $A \equiv 0$ or $1 \pmod 4$, then $C_2 = 1$. If $A \equiv 3 \pmod 4$, then $C_2 = 2$. When $A \equiv 2 \pmod 4$, the situation is more complicated, and we summarise the value C_2 modulo 2 according to $A \pmod{128}$ as follows.

$A \bmod 128$	2	6	10	14	18	22	26	30	34	38	42
$C_2 \bmod 2$	0	0	1	0	0	0	1	1	0	0	1
$A \bmod 128$	46	50	54	58	62	66	70	74	78	82	86
$C_2 \bmod 2$	0	0	0	1	1	0	0	1	0	0	0
$A \bmod 128$	90	94	98	102	106	110	114	118	122	126	
$C_2 \bmod 2$	1	1	0	0	1	0	0	0	1		

If $A \equiv 126 \pmod{128}$*, then the parity of* C_2 *is the same as the parity of* $\mathrm{ord}_2(A+2)$*. Moreover,* E *has good reduction modulo 2 if and only if* $A \equiv 62 \pmod{128}$*. In particular,* C_2 *is odd if and only if* $A \equiv 0 \pmod 4$*;* $A \equiv 1 \pmod 4$*;* $A \equiv 10 \pmod{16}$*;* $A \equiv 62 \pmod{128}$*; or* $A \equiv 126 \pmod{128}$ *and* $\mathrm{ord}_2(A+2)$ *is odd.*

(ii) Suppose that $B = -1$*. Then* C_2 *is even if and only if* $A \equiv 0 \pmod 4$*.*

Proof. Tate's algorithm. □

Remark. By Propositions 4.32 and 4.33, we assume the following throughout this section; E is an elliptic curve defined by the equation (4.16) for relatively prime $A \in \mathbf{Z}$ and $B \in \{1, -1, 16, -16\}$ with discriminant $\Delta = 2^4B^2(A^2 - 4B)$, such that all odd prime divisors of $A^2 - 4B$ has odd exponent. Moreover,

- when $B = 1$, we assume $A \equiv 0 \pmod 4$, $A \equiv 1 \pmod 4$, $A \equiv 10 \pmod{16}$, $A \equiv 62 \pmod{128}$, or $A \equiv 126 \pmod{128}$ and $\mathrm{ord}_2(A+2)$ is odd;
- when $B = -1$, we assume $A \not\equiv 0 \pmod 4$;
- when $B = \pm 16$, we assume $A \equiv 1 \pmod 4$.

Remark. We furthermore assume $\Delta > 0$, by removing finitely many exceptional cases by explicit computation. As $\Delta = 16B^2(A^2 - 4B)$, we need to check the cases $(A, B) = (0, 1)$, $(\pm 1, 1)$ and $(\pm n, 16)$ for $n = 0, 1, \cdots, 7$. This is easy with Sage Mathematics Software [SAGE].

4.7.2 $(\#Ш(E/K))^{1/2}$

In this subsection, we shall see $2 \mid (\#Ш(E/K))^{1/2}$, for various remaining cases left from considerations about Tamagawa numbers. Our main job is to show $\sum i_\ell + \dim \Phi \geq 4$ (notations from subsection 4.3.1). Then,

$$\boxed{\sum i_\ell + \dim \Phi \geq 4} \Longrightarrow \boxed{\dim_{\mathbf{F}_2} Ш(E/K)[2] \geq 1} \Longrightarrow \boxed{2 \mid (\#Ш(E/K))^{1/2}}.$$

The first implication follows from Kramer's theorem (see subsection 4.3.1), and the last implication is due to Kolyvagin's theorem [Kol].

Proposition 4.34. *Suppose that $B = 1$. Then we have $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$, i.e., $2 \mid (\#Ш(E/K))^{1/2}$, except for '17a3', '32a3', and '80a2', for which $2 \mid M$.*

Proof. Our elliptic curve E is given by

$$y^2 = x^3 + Ax^2 + x, \tag{4.17}$$

where $A \equiv 0 \pmod 4$, $A \equiv 1 \pmod 4$, $A \equiv 10 \pmod{16}$, $A \equiv 30 \pmod{32}$, or $A \equiv 62 \pmod{128}$; having discriminant $\Delta = 16(A^2 - 4)$. This is minimal except possibly at 2. E has good reduction modulo 2 if and only if $A \equiv 62 \pmod{128}$. The minimal discriminant of E is given by $\Delta_{\min} = \begin{cases} 2^{-12}\Delta & \text{if } A \equiv 62 \pmod{64}, \\ \Delta & \text{otherwise} \end{cases}$. Note that we have assumed $\Delta_{\min} > 0$.

We divide the proof into three parts: (i) when E has good reduction modulo 2, (ii) when $A \equiv 126 \pmod{128}$ and $\mathrm{ord}_2\left(2^{-8}\left(A^2 - 4\right)\right)$ is odd, and (iii) other cases.

Case (i) E has good reduction modulo 2, i.e., $A \equiv 62 \pmod{128}$. In this case, the minimal discriminant of E is given by $\Delta_{\min} = 2^{-8}(A^2 - 4)$. In order to clarify the group $\mathrm{Sel}^\phi(E/\mathbf{Q})$, we look at local images as follows.

- $\mathrm{im}\,\delta_\infty = \begin{cases} \mathbf{R}^\times/\mathbf{R}^{\times 2} & \text{if } A < 0, \\ \{1\} & \text{if } A > 0. \end{cases}$
- $\mathrm{im}\,\delta_p = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \nmid \Delta$.
- $\mathrm{im}\,\delta_p = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for odd primes $p \mid \Delta$.
- $\mathrm{im}\,\delta_2 = \mathbf{Z}_2^\times \mathbf{Q}_2^{\times 2}/\mathbf{Q}_2^{\times 2} = \{\pm 1, \pm 5\}$.

Thus $\mathrm{Sel}^\phi(E/\mathbf{Q}) = \begin{cases} \langle -1, p : p \mid \Delta \rangle & \text{if } A < 0 \\ \langle p : p \mid \Delta \rangle & \text{if } A > 0 \end{cases}$. Considering the factorisation $A^2 - 4 = (A-2)(A+2)$, we always choose at least two distinct odd primes dividing $A^2 - 4$, except for the curve '17a3' (when $A = -66$), in which case $M = 2$. Excluding this, in the sequel, we assume $A^2 - 4$ has at least two odd prime divisors.

Let d be a negative, square-free integer. We now compute the sum of local norm indices $\sum i_\ell$. Note that $i_\infty = 1$. After excluding obvious cases giving $\sum i_\ell \geq 4$, we have the following four cases:

- $d = -2$;
- $d = -q$ for an odd prime q;
- $d = -2q$ for an odd prime q;
- $d = -qq'$ for odd primes q, q'.

First, let $d = -2$. Local images of the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$ are given as follows.

- $\mathrm{im}\,\delta_\infty^d = \begin{cases} \mathbf{R}^\times/\mathbf{R}^{\times 2} & \text{if } A > 0, \\ \{1\} & \text{if } A \le 0. \end{cases}$
- $\mathrm{im}\,\delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \nmid \Delta$.
- $\mathrm{im}\,\delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \mid \Delta$.
- $\mathrm{im}\,\delta_2^d = \langle 2, -5, c\rangle$, where $c = (A^2-4)/4$.

Write $A = 62 + 128k$ for some $k \in \mathbf{Z}$. Note that $A^2 - 4 = 2^8(32k+15)(2k+1)$, and that $\gcd(32k+15, 2k+1) = 1$.

- If $k \equiv 0 \pmod 4$, then $(\Delta_{\min}, d)_{\mathbf{Q}_2} = \left(2^{-8}(A^2-4), -2\right)_{\mathbf{Q}_2} = (-1,-2)_{\mathbf{Q}_2} = -1$, so $\sum i_\ell = i_\infty + i_2 = 2$. In this case $c = (A^2-4)/4 = -1 \in \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$, and thus $\mathrm{im}\,\delta_2^d = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$. Suppose that there are exactly two odd prime divisors dividing Δ. Considering Heegner hypothesis, then we must have $32k + 15 = -p^a$ for some prime $p \equiv 1 \pmod 8$ and odd a. Then, as $k \equiv 0 \pmod 4$ and $k < 0$, the another odd prime dividing $2k+1$ must be congruent to -1 modulo 8, a contradiction to Heegner hypothesis. Hence, there must be at least 3 odd primes dividing Δ, and if we choose two of them, say, p_1 and p_2, then their images in Φ are distinct and non-trivial, i.e., $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \ge 4$.
- If $k \equiv 1 \pmod 4$, then $(\Delta_{\min}, d)_{\mathbf{Q}_2} = \left(2^{-8}(A^2-4), -2\right)_{\mathbf{Q}_2} = (5,-2)_{\mathbf{Q}_2} = -1$, so $\sum i_\ell = 2$. In this case $c = (A^2-4)/4 = 5 \in \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$, and thus $\mathrm{im}\,\delta_2^d = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$. Similar as above, there must be at least 3 odd primes dividing Δ, and we have $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \ge 4$.

- If $k \equiv 2$ or $3 \pmod 4$, then $(\Delta_{\min}, d)_{\mathbf{Q}_2} = \left(2^{-8}(A^2-4), -2\right)_{\mathbf{Q}_2} = 1$, so $\sum i_\ell = 3$. In this case $\operatorname{im} \delta_2^d = \{1, 2, -5, 10\}$. However, by Heegner condition, any odd prime p dividing Δ must have $p \equiv 1$ or $-5 \pmod 8$. We are done because there must be at least two odd primes dividing Δ.

Suppose that $d = -q$ with $q \equiv 1 \pmod 4$, i.e., $d \equiv 3 \pmod 4$. In this case the prime 2 is ramified in K. As $d \equiv -1$ or $-5 \pmod 8$, it is safe to assume $\Delta_{\min} \equiv -1$ or $-5 \pmod 8$, since otherwise we have $\sum i_\ell \geq 4$. Moreover, for i_q, we assume $\left(\dfrac{A^2-4}{q}\right) = -1$, since otherwise we have $i_q = 2$ and thus $\sum i_\ell \geq 4$. We have $\sum i_\ell = 3$. Local images for the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$ are given as follows.

- $\operatorname{im} \delta_\infty^d = \begin{cases} \mathbf{R}^\times/\mathbf{R}^{\times 2} & \text{if } A > 0, \\ \{1\} & \text{if } A \leq 0. \end{cases}$
- $\operatorname{im} \delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \nmid \Delta q$.
- $\operatorname{im} \delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \mid \Delta q$.
- $\operatorname{im} \delta_2^d = \mathbf{Z}_2^\times \mathbf{Q}_2^{\times 2}/\mathbf{Q}_2^{\times 2} = \{\pm 1, \pm 5\}$.

As the image of an odd prime $p \mid \Delta$ in Φ is non-trivial, we have $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$.

Suppose that $q \equiv 3 \pmod 4$, i.e., $d = -q \equiv 1 \pmod 4$. In this case the prime 2 in $\mathbf{Q}$ is unramified in K. We have $i_\infty = 1$ and $i_2 = 0$. Local images for the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$ are given as follows.

- $\operatorname{im} \delta_\infty^d = \begin{cases} \mathbf{R}^\times/\mathbf{R}^{\times 2} & \text{if } A > 0, \\ \{1\} & \text{if } A \leq 0. \end{cases}$
- $\operatorname{im} \delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \nmid \Delta q$.
- $\operatorname{im} \delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \mid \Delta$.
- $\operatorname{im} \delta_q^d = \begin{cases} \{1, qu\} & \text{if } q \nmid A \text{ and } \left(\frac{A^2-4}{q}\right) = 1, \text{ for some } u \in \mathbf{Z}_q^\times, \\ \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{otherwise.} \end{cases}$
- $\operatorname{im} \delta_2^d = \mathbf{Z}_2^\times \mathbf{Q}_2^{\times 2}/\mathbf{Q}_2^{\times 2} = \{\pm 1, \pm 5\}$.

For any odd prime $p \mid \Delta$, by Heegner hypothesis, we have $1 = \left(\frac{-q}{p}\right) = \left(\frac{p}{q}\right)$. Hence we always have $\left(\frac{A^2-4}{q}\right) = 1$, i.e., $i_q = 2$. We must have $\dim_{\mathbf{F}_2} \Phi \geq 1$ by considering the image of one of such odd $p \mid \Delta$ in Φ, whence $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$.

Suppose that $d = -2q$ for some odd prime q. In this case, we can moreover assume that $\left(\frac{A^2-4}{q}\right) = -1$, since otherwise we have $\sum i_\ell \geq 4$. Write $c = A^2 - 4$. For the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$, we look at the local images.

- $\operatorname{im} \delta_\infty^d = \begin{cases} \mathbf{R}^\times/\mathbf{R}^{\times 2} & \text{if } A > 0, \\ \{1\} & \text{if } A \leq 0. \end{cases}$
- $\operatorname{im} \delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \nmid \Delta q$.
- $\operatorname{im} \delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \mid \Delta$.
- $\operatorname{im} \delta_q^d = \begin{cases} \{1, qu\} & \text{if } q \mid A \text{ and } q \equiv 1 \pmod 4, \text{ for some } u \in \mathbf{Z}_q^\times, \\ \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{otherwise.} \end{cases}$
- $\operatorname{im} \delta_2^d = \begin{cases} \langle 2, -5, c\rangle & \text{when } q \equiv 1 \pmod 8, \\ \langle -1, 2, c\rangle & \text{when } q \equiv -1 \pmod 8, \\ \langle -2, -5, c\rangle & \text{when } q \equiv 5 \pmod 8, \\ \langle -1, 10, c\rangle & \text{when } q \equiv -5 \pmod 8. \end{cases}$

Now we are going to do some case-by-case study. First, we know $c = A^2 - 4$ is *exactly* divisible by 2^8, we let $c' = 2^{-8}c = \Delta_{\min}$.

(i) Suppose that $q \equiv 1 \pmod 8$. Then $d = -2$ in $\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

  (i) If $c' \equiv 1 \pmod 8$, then $(d, \Delta_{\min})_{\mathbf{Q}_2} = 1$, and thus $i_2 = 2$, i.e., $\sum i_\ell = 4$.

  (ii) If $c' \equiv -1 \pmod 8$, then $(d, \Delta_{\min})_{\mathbf{Q}_2} = -1$, and thus $i_2 = 1$, i.e., $\sum i_\ell = 3$. In this case $\operatorname{im} \delta_2^d = \langle 2, -5, -1\rangle = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

  (iii) If $c' \equiv 5 \pmod 8$, then $(d, \Delta_{\min})_{\mathbf{Q}_2} = -1$, and thus $i_2 = 1$, i.e., $\sum i_\ell = 3$. In this case $\operatorname{im} \delta_2^d = \langle 2, -5, 5\rangle = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

(iv) If $c' \equiv -5 \pmod 8$, then $(d, \Delta_{\min})_{\mathbf{Q}_2} = 1$, and thus $i_2 = 2$, i.e., $\sum i_\ell = 4$.

(ii) Suppose that $q \equiv -1 \pmod 8$. Then $d = 2$ in $\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

(i) If $c' \equiv 1 \pmod 8$, then $(d, \Delta_{\min})_{\mathbf{Q}_2} = 1$, and thus $i_2 = 2$, i.e., $\sum i_\ell = 4$.

(ii) If $c' \equiv -1 \pmod 8$, then $(d, \Delta_{\min})_{\mathbf{Q}_2} = 1$, and thus $i_2 = 2$, i.e., $\sum i_\ell = 4$.

(iii) If $c' \equiv 5 \pmod 8$, then $(d, \Delta_{\min})_{\mathbf{Q}_2} = -1$, and thus $i_2 = 1$, i.e., $\sum i_\ell = 3$. In this case $\operatorname{im} \delta_2^d = \langle -1, 2, 5\rangle = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

(iv) If $c' \equiv -5 \pmod 8$, then $(d, \Delta_{\min})_{\mathbf{Q}_2} = -1$, and thus $i_2 = 1$, i.e., $\sum i_\ell = 3$. In this case $\operatorname{im} \delta_2^d = \langle -1, 2, -5\rangle = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

(iii) Suppose that $q \equiv 5 \pmod 8$. Then $d = -10$ in $\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

(i) If $c' \equiv 1 \pmod 8$, then $(d, \Delta_{\min})_{\mathbf{Q}_2} = 1$, and thus $i_2 = 2$, i.e., $\sum i_\ell = 4$.

(ii) If $c' \equiv -1 \pmod 8$, then $(d, \Delta_{\min})_{\mathbf{Q}_2} = -1$, and thus $i_2 = 1$, i.e., $\sum i_\ell = 3$. In this case $\operatorname{im} \delta_2^d = \langle -2, -5, -1\rangle = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

(iii) If $c' \equiv 5 \pmod 8$, then $(d, \Delta_{\min})_{\mathbf{Q}_2} = -1$, and thus $i_2 = 1$, i.e., $\sum i_\ell = 3$. In this case $\operatorname{im} \delta_2^d = \langle -2, -5, 5\rangle = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

(iv) If $c' \equiv -5 \pmod 8$, then $(d, \Delta_{\min})_{\mathbf{Q}_2} = 1$, and thus $i_2 = 2$, i.e., $\sum i_\ell = 4$.

(iv) Suppose that $q \equiv -5 \pmod 8$. Then $d = 10$ in $\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

(i) If $c' \equiv 1 \pmod 8$, then $(d, \Delta_{\min})_{\mathbf{Q}_2} = 1$, and thus $i_2 = 2$, i.e., $\sum i_\ell = 4$.

(ii) If $c' \equiv -1 \pmod 8$, then $(d, \Delta_{\min})_{\mathbf{Q}_2} = 1$, and thus $i_2 = 2$, i.e., $\sum i_\ell = 4$.

(iii) If $c' \equiv 5 \pmod 8$, then $(d, \Delta_{\min})_{\mathbf{Q}_2} = -1$, and thus $i_2 = 1$, i.e., $\sum i_\ell = 3$. In this case $\operatorname{im} \delta_2^d = \langle -1, 10, 5\rangle = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

(iv) If $c' \equiv -5 \pmod 8$, then $(d, \Delta_{\min})_{\mathbf{Q}_2} = -1$, and thus $i_2 = 1$, i.e., $\sum i_\ell = 3$. In this case $\operatorname{im} \delta_2^d = \langle -1, 10, -5\rangle = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

Having these discussions, we can conclude that we have either $\sum i_\ell = 4$ or $\operatorname{im} \delta_2^d = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$. Thus, we have $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$.

Suppose that $d = -qq'$ for some distinct odd primes q and q'. If the prime 2 is ramified in $K = \mathbf{Q}(\sqrt{d})$ then we have $\sum i_\ell \geq 4$. So we can assume $d \equiv 1 \pmod 4$,

which means, without loss of generality, $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$. Moreover, if either $\left(\frac{A^2-4}{q}\right) = 1$ or $\left(\frac{A^2-4}{q'}\right) = 1$, then we have $\sum i_\ell \geq 4$ again, and thus we somewhat strictly assume $\left(\frac{A^2-4}{q}\right) = \left(\frac{A^2-4}{q'}\right) = -1$. Note also that $qq' \equiv -1$ or $-5 \pmod 8$. The local images for the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$ are given as follows.

- $\mathrm{im}\,\delta_\infty^d = \begin{cases} \mathbf{R}^\times/\mathbf{R}^{\times 2} & \text{if } A > 0, \\ \{1\} & \text{if } A \leq 0. \end{cases}$
- $\mathrm{im}\,\delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \nmid \Delta qq'$.
- $\mathrm{im}\,\delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \mid \Delta q'$.
- $\mathrm{im}\,\delta_q^d = \begin{cases} \{1, qu\} & \text{if } q \mid A, \text{ for some } u \in \mathbf{Z}_q^\times, \\ \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{otherwise.} \end{cases}$
- $\mathrm{im}\,\delta_2^d = \mathbf{Z}_2^\times \mathbf{Q}_2^{\times 2}/\mathbf{Q}_2^{\times 2}$

By Heegner hypothesis, for each odd prime $p \mid \Delta$, $1 = \left(\frac{-qq'}{p}\right) = \left(\frac{p}{q}\right)\left(\frac{p}{q'}\right)$. Since $\left(\frac{A^2-4}{q}\right) = \left(\frac{A^2-4}{q'}\right) = -1$, if there are exactly two odd primes dividing Δ, then we can always take an odd prime $p \mid \Delta$ such that $\left(\frac{p}{q}\right) = 1$. Then the image of p in Φ yields $\dim_{\mathbf{F}_2} \Phi \geq 1$. If there are at least 3 odd primes dividing Δ and $\left(\frac{p}{q}\right) = -1$ for all odd prime $p \mid \Delta$, then we may choose two such primes pp' and consider the image of pp' in Φ. In any case we have $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$.

Case (ii) when $A \equiv 126 \pmod{128}$ and $\mathrm{ord}_2\left(2^{-8}\left(A^2-4\right)\right)$ is odd. In this case the minimal discriminant of $E/\mathbf{Q}$ is $\Delta_{\min} = 2^{-8}(A^2-4)$. In particular, E has bad reduction modulo 2. If we write $A = 126 + 128k$ for some $k \in \mathbf{Z}$, then $\Delta_{\min} = 2(32k+31)(k+1)$. So the condition "$\mathrm{ord}_2\left(2^{-8}\left(A^2-4\right)\right)$ is odd" can be translated into "$\mathrm{ord}_2(k+1)$ being even". There must be at least one odd prime dividing Δ since otherwise we have $\Delta = 0$.

By the Heegner condition, we must have either $d = -q$ with $q \equiv -1 \pmod 8$ or $d = -qq'$ with $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$, also, in any case we must have $d \equiv 1 \pmod 8$. We now compute the Selmer group $\mathrm{Sel}^{\phi}(E/\mathbf{Q})$. From [Got], the local images are given as follows.

- $\mathrm{im}\,\delta_\infty = \begin{cases} \mathbf{R}^\times/\mathbf{R}^{\times 2} & \text{if } A < 0, \\ \{1\} & \text{if } A \geq 0. \end{cases}$.
- $\mathrm{im}\,\delta_p = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \nmid \Delta$.
- $\mathrm{im}\,\delta_p = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for odd primes $p \mid \Delta$.
- $\mathrm{im}\,\delta_2 = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

Now suppose that $d = -q$ with $q \equiv -1 \pmod 8$. For $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$, we have the following local images.

- $\mathrm{im}\,\delta_\infty^d = \begin{cases} \mathbf{R}^\times/\mathbf{R}^{\times 2} & \text{if } A > 0, \\ \{1\} & \text{if } A \leq 0. \end{cases}$
- $\mathrm{im}\,\delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \nmid \Delta q$.
- $\mathrm{im}\,\delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \mid \Delta$.
- $\mathrm{im}\,\delta_q^d = \begin{cases} \{1, qu\} & \text{if } q \nmid A \text{ and } \left(\frac{A^2-4}{q}\right) = 1, \text{ for some } u \in \mathbf{Z}_q^\times, \\ \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{otherwise.} \end{cases}$
- $\mathrm{im}\,\delta_2^d = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

Let p be an odd prime dividing Δ. By Heegner condition, the primes 2 and p must split completely in K, and thus we must have $q \equiv -1 \pmod 8$ and $\left(\frac{p}{q}\right) = \left(\frac{-q}{p}\right) = 1$. Then, we can see that $\left(\frac{A^2-4}{q}\right) = 1$, whence $i_q = 2$. Since $\left(\frac{2}{q}\right) = 1$, the image of the prime 2 is contained in Φ and is non-trivial, we have $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$.

Suppose that $d = -qq'$ with $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$. More precisely, considering Heegner hypothesis, we have $d \equiv 1 \pmod 8$, and thus either $(q, q') \equiv$

$(1,-1) \pmod 8$ or $(q,q') \equiv (5,-5) \pmod 8$. We assume $\left(\frac{A^2-4}{q}\right) = \left(\frac{A^2-4}{q'}\right) = -1$, so that $\sum i_\ell = 3$. For the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$, we have the following local images.

- $\mathrm{im}\,\delta_\infty^d = \begin{cases} \mathbf{R}^\times/\mathbf{R}^{\times 2} & \text{if } A > 0, \\ \{1\} & \text{if } A \le 0. \end{cases}$
- $\mathrm{im}\,\delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \nmid \Delta q q'$.
- $\mathrm{im}\,\delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \mid \Delta q'$.
- $\mathrm{im}\,\delta_q^d = \begin{cases} \{1, qu\} & \text{if } q \mid A, \text{ for some } u \in \mathbf{Z}_q^\times, \\ \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{otherwise.} \end{cases}$
- $\mathrm{im}\,\delta_2^d = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.

If $\left(\frac{2}{q}\right) = 1$, i.e., $q \equiv 1 \pmod 8$, then the image of 2 must be in Φ, and is non-trivial. If $\left(\frac{2}{q}\right) = -1$ and there is exactly one odd prime $p \mid \Delta$, then by the condition $\left(\frac{A^2-4}{q}\right) = -1$, p is a quadratic residue modulo q, and thus the image of p is contained in Φ and is non-trivial. If there are at least 2 odd primes dividing Δ, then there always is a prime $p \mid \Delta$ such that either p or $2p$ is a quadratic residue modulo q. In any cases, we always have $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \ge 4$.

Case (iii) the remaining cases. As noted above, the remaining cases are again subdivided into the following cases:

- $A \equiv 0 \pmod 4$,
- $A \equiv 1 \pmod 4$, or
- $A \equiv 10, 26, 30, 42, 58 \pmod{64}$.

The minimal discriminant of $E/\mathbf{Q}$ is given by $\Delta_{\min} = 2^4(A^2-4)$. In this case the prime 2 is always bad. So by the Heegner condition, d must be congruent to 1 modulo

8. This implies that $i_2 = 0$. As we noted $i_\infty = 1$, we must have either $d = -q$ with $q \equiv -1 \pmod 8$ or $d = -qq'$ with $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$. Note also that by considering factorisations of $A^2 - 4$ for the various cases, we can conclude that there is at least one odd prime dividing Δ, except for $A = -6$. However, when $A = -6$, the curve E is '32a3', having $M = 2$, so we can safely exclude this curve. Moreover, if $A \equiv 1 \pmod 4$ and if there is only one odd prime dividing Δ, then under the condition $\Delta > 0$, A must be -3 or ± 4. These correspond to the single curve '80a2', having $M = 2$. So whenever we deal with the case $A \equiv 1 \pmod 4$, we further assume that there are at least two odd primes dividing Δ.

We now compute the Selmer group $\mathrm{Sel}^{\phi}(E/\mathbf{Q})$. From [Got], note the following local images.

- $\mathrm{im}\,\delta_\infty = \begin{cases} \mathbf{R}^\times/\mathbf{R}^{\times 2} & \text{if } A < 0, \\ \{1\} & \text{if } A \geq 0. \end{cases}$.
- $\mathrm{im}\,\delta_p = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \nmid \Delta$.
- $\mathrm{im}\,\delta_p = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for odd primes $p \mid \Delta$.
- $\mathrm{im}\,\delta_2 = \begin{cases} \mathbf{Z}_2^\times \mathbf{Q}_2^{\times 2}/\mathbf{Q}_2^{\times 2} & \text{if } A \equiv 1 \pmod 4, \\ \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2} & \text{if } A \text{ is even.} \end{cases}$

Suppose first that $d = -q$ with $q \equiv -1 \pmod 8$. For $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$, we have the following local images.

- $\mathrm{im}\,\delta_\infty^d = \begin{cases} \mathbf{R}^\times/\mathbf{R}^{\times 2} & \text{if } A > 0, \\ \{1\} & \text{if } A \leq 0. \end{cases}$
- $\mathrm{im}\,\delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \nmid \Delta q$.
- $\mathrm{im}\,\delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \mid \Delta$.
- $\mathrm{im}\,\delta_q^d = \begin{cases} \{1, qu\} & \text{if } q \nmid A \text{ and } \left(\frac{A^2-4}{q}\right) = 1, \text{ for some } u \in \mathbf{Z}_q^\times, \\ \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{otherwise.} \end{cases}$

- $\operatorname{im} \delta_2^d = \begin{cases} \mathbf{Z}_2^\times \mathbf{Q}_2^{\times 2}/\mathbf{Q}_2^{\times 2} & \text{if } A \equiv 1 \pmod 4, \\ \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2} & \text{if } A \text{ is even.} \end{cases}$.

Now we adopt the Heegner condition. If p is an odd prime dividing A^2-4, then $1 = \left(\frac{-q}{p}\right) = \left(\frac{p}{q}\right)$. Thus $\left(\frac{A^2-4}{q}\right) = 1$, and $i_q = 2$, i.e., $\sum i_\ell = 3$. When $A \equiv 1 \pmod 4$, then the image of any odd prime $p \mid \Delta$ is contained in Φ and is non-trivial. On the other hand when A is even, the image of 2 is contained in Φ and is non-trivial, since 2 is a quadratic residue modulo q. Thus $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$ in any cases.

Suppose that $d = -qq'$ with $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$. More precisely, considering Heegner hypothesis, we have $d \equiv 1 \pmod 8$, and thus either $(q, q') \equiv (1, -1) \pmod 8$ or $(q, q') \equiv (5, -5) \pmod 8$. We only need to consider the cases when $\left(\frac{A^2-4}{q}\right) = \left(\frac{A^2-4}{q'}\right) = -1$, i.e., $\sum i_\ell = 3$. For the Selmer group $\operatorname{Sel}^{\phi_d}(E_d/\mathbf{Q})$, we have the following local images.

- $\operatorname{im} \delta_\infty^d = \begin{cases} \mathbf{R}^\times/\mathbf{R}^{\times 2} & \text{if } A > 0, \\ \{1\} & \text{if } A \leq 0. \end{cases}$
- $\operatorname{im} \delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \nmid \Delta q q'$.
- $\operatorname{im} \delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \mid \Delta q'$.
- $\operatorname{im} \delta_q^d = \begin{cases} \{1, qu\} & \text{if } q \mid A, \text{ for some } u \in \mathbf{Z}_q^\times, \\ \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times 2} & \text{otherwise.} \end{cases}$
- $\operatorname{im} \delta_2^d = \begin{cases} \mathbf{Z}_2^\times \mathbf{Q}_2^{\times 2}/\mathbf{Q}_2^{\times 2} & \text{if } A \equiv 1 \pmod 4, \\ \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2} & \text{if } A \text{ is even.} \end{cases}$

If $A \equiv 1 \pmod 4$, then by the condition $\left(\frac{A^2-4}{q}\right) = -1$, we can choose a representative $x \in \mathbf{Z}$ which is either an odd prime dividing Δ or a product of two primes dividing Δ, such that x is a quadratic residue modulo q. If $A \equiv 0 \pmod 4$, then we can find two distinct odd primes dividing Δ except for the cases $A = \pm 4$. If $A \neq \pm 4$, then we choose x to be either 2 or $2p$ with an odd prime $p \mid \Delta$ such

that x is a quadratic residue modulo q. This is always possible by the condition $\left(\frac{A^2-4}{q}\right) = -1$. If $A = \pm 4$, then we do not have $q \mid A$. This means that we do not need to consider whether x is a quadratic residue or not. In this case just take $x = 2$. If A is one of remaining cases, we take x to be a prime $p \mid \Delta$, such that p is a quadratic residue modulo q. This is always possible since $A^2 - 4$ is a quadratic non-residue modulo q. Now, in any cases, the image of x is contained in Φ and is non-trivial. Thus $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$. □

Proposition 4.35. *Suppose that $B = -1$. By the considerations of the subsection above, we assume*

- $A \equiv 0 \pmod 4$, *and*
- *if ℓ is an odd prime dividing $A^2 - 4B = A^2 + 4$, then it has odd exponent.*

Then we have $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$, i.e., $2 \mid (\#Ш(E/K))^{1/2}$, except for

- *'128b2' and '128d2', for which $2 \mid M$;*
- *a family of curves for which $A^2 + 4$ is a power of a prime number.*

Remark. The exceptional family will be dealt with in the next subsection 4.7.3.

Proof. Our elliptic curve E is given by

$$y^2 = x^3 + Ax^2 - x, \tag{4.18}$$

such that $A \equiv 1, 2, 3 \pmod 4$. In any cases, the minimal discriminant of the curve becomes $\Delta_{\min} = \Delta = 2^4(A^2 + 4)$. In particular, the prime 2 is always a bad one. Since 2 must split comletely in K, we must have $d \equiv 1 \pmod 8$. Since $i_q \geq 1$ for each prime divisor q of d, we may assume that there are at most 2 prime divisors in d, as $i_\infty = 1$ always. Glueing this with the fact that $d \equiv 1 \pmod 8$, we have either $d = -q$ for an odd prime q such that $q \equiv -1 \pmod 8$ or $d = -qq'$, for distinct odd primes q and q' such that $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$ with either $(q, q') \equiv (1, -1) \pmod 8$ or $(q, q') \equiv (5, -5) \pmod 8$.

If ℓ is an odd prime dividing Δ, i.e., $\ell \mid \left(A^2 + 4\right)$, then by the "sum of two squares" theorem, we must have $\ell \equiv 1 \pmod 4$, i.e., $\ell \equiv 1$ or $5 \pmod 8$.

Now we compute the group $\mathrm{Sel}^{\phi}(E/\mathbf{Q})$. Note the following local images. Definitions for δ_ℓ are the same as in §4.6.

- $\operatorname{im}\delta_\infty = \{1\}$.
- $\operatorname{im}\delta_p = \mathbf{Z}_p\mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$, for odd primes $p \nmid \Delta$.
- $\operatorname{im}\delta_p = \mathbf{Q}_p^{\times}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \mid \Delta$.
- $\operatorname{im}\delta_2 = \begin{cases} \{1,5\} & \text{if } A \equiv 1,3 \pmod 4, \\ \{1,2,5,10\} & \text{if } A \equiv 2 \pmod 4. \end{cases}$

Suppose that $d = -q$ with $q \equiv -1 \pmod 8$ Since $\left(\frac{-q}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$, we have $\left(\frac{p}{q}\right) = 1$ for any odd prime $p \mid (A^2+4)$. If $A \equiv 1,3 \pmod 4$, then A^2+4 is odd, and as every prime divisor of A^2+4 has odd exponent, we can conclude that $\left(\frac{A^2+4}{q}\right) = 1$ because the left hand side of the expression is the product of $\left(\frac{p}{q}\right)$ running over all primes $p \mid (A^2+4)$. Secondly, suppose that $A \equiv 2 \pmod 4$. This means that there is an integer k such that $A = 2+4k$, whence $A^2+4 = 16k^2+16k+8 = 2^3(2k^2+2k+1)$, so $\operatorname{ord}_2(A^2+4) = 3$. In this case, $\left(\frac{A^2+4}{q}\right) = \left(\frac{2}{q}\right)\prod_{\substack{p \text{ odd primes,} \\ p \mid A^2+4}}\left(\frac{p}{q}\right) = 1$, since $q \equiv -1 \pmod 8$. Therefore, we always have $\left(\frac{A^2+4}{q}\right) = 1$, i.e., $i_q = 2$, whence $\sum i_\ell = 3$.

Now consider the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$. The local images are given as follows.

- $\operatorname{im}\delta_\infty^d = \{1\}$.
- $\operatorname{im}\delta_p^d = \mathbf{Z}_p\mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$, for odd primes $p \nmid \Delta q$.
- $\operatorname{im}\delta_p^d = \mathbf{Q}_p^{\times}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \mid \Delta$.
- $\operatorname{im}\delta_q^d = \{1\}$.

- $\mathrm{im}\,\delta_2^d = \begin{cases} \{1,5\} & \text{if } A \equiv 1,3 \pmod 4, \\ \{1,2,5,10\} & \text{if } A \equiv 2 \pmod 4. \end{cases}$

If $A \equiv 2 \pmod 4$ then $\mathrm{ord}_2(A^2+4) = 3$. As 2 is a quadratic residue modulo q, and since A^2+4 must have at least one odd prime except for the cases $A = \pm 2$, the image of 2 gives a nontrivial element in Φ. When $A = \pm 2$, the curve is equal to '128b2' or '128d2'. In these cases $M = 2$. If $A \equiv 1$ or $3 \pmod 4$ and if there are at least two prime divisors of A^2+4, then we can also find a nontrivial element in Φ. If A^2+4 is a power of a prime, then this will be dealt as exceptional cases. See 4.7.3.

Suppose that $d = -qq'$ with $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$. First note that we are reduced to the case that $\left(\frac{A^2+4}{q}\right) = \left(\frac{A^2+4}{q'}\right) = -1$, since otherwise we have $\sum i_\ell \geq 4$. Moreover, if $\ell \mid A$, for $\ell = q$ or q' then we have $\left(\frac{A^2+4}{\ell}\right) = \left(\frac{4}{\ell}\right) = 1$, a contradiction. Now we impose the Heegner hypothesis. At first, since the prime 2 must split completely in K, so thus $d \equiv 1 \pmod 8$, and we have $(q, q') \equiv (1,-1)$ or $\equiv (5,-5) \pmod 8$. For odd primes p dividing Δ, we must have $p \equiv 1 \pmod 4$ by 'sum of two squares theorem', and thus we have to have either $\left(\frac{p}{q}\right) = \left(\frac{p}{q'}\right) = 1$ or $\left(\frac{p}{q}\right) = \left(\frac{p}{q'}\right) = -1$.

Local images for the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$ are given as follows:

- $\mathrm{im}\,\delta_\infty^d = \{1\}$;
- $\mathrm{im}\,\delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$, for odd primes $p \nmid \Delta q$ (including $p = q'$);
- $\mathrm{im}\,\delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$, for odd primes $p \mid \Delta q$;
- $\mathrm{im}\,\delta_2^d = \begin{cases} \{1,5\} & \text{when } A \equiv 1,3 \pmod 4, \\ \{1,2,5,10\} & \text{when } A \equiv 2 \pmod 4. \end{cases}$

Similar as above, if $A \equiv 2 \pmod 4$, then the image of 2 in Φ is a non-trivial element, so that $\dim_{\mathbf{F}_2} \Phi \geq 1$. Now assume A is odd. If A^2+4 have at least two distinct odd prime divisor, then the image of either one of them gives a non-trivial element in Φ. If A^2+4 is a power of a prime, then this will be dealt as exceptional cases. See 4.7.3. □

Proposition 4.36. *Suppose that $B = 16$. Then we have $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$, i.e., $2 \mid (\#Ш(E/K))^{1/2}$, except for '17a4', for which $2 \mid M$.*

Proof. Our elliptic curve E is given by

$$y^2 = x^3 + Ax^2 + 16x, \tag{4.19}$$

such that $A \equiv 1 \pmod 4$. The discriminant is $\Delta = 2^{12}\left(A^2 - 64\right)$, whereas the minimal discriminant of the curve is given by $\Delta_{\min} = 2^{-12}2^4(2^4)^2(A^2 - 4 \cdot 2^4) = A^2 - 2^6 = (A + 2^3)(A - 2^3)$. In particular, note that the prime 2 is always a good prime for E. We have assumed that $\Delta_{\min} = A^2 - 64 > 0$, for the other finitely many cases can be dealt by computing explicitly.

Note that there are at least two odd primes dividing $A^2 - 64$, except for the curve '17a4', which has Manin constant 4. This can be seen by considering the factorisation of $A^2 - 64$. So from now on, we assume that there are always at least two distinct odd primes dividing $A^2 - 64$.

Now we are going to compute local norm indices. It is clear that $i_\infty = 1$. Having the above proposition, when the prime 2 is ramified in K, we have $i_2 = 1$ or 2 according to $(\Delta_{\min}, d)_{\mathbf{Q}_2} = 1$ or -1. Thus we may assume either one of the following cases:

- $d = -2$;
- $d = -q$, for an odd prime q;
- $d = -2q$, for an odd prime q;
- $d = -qq'$, for odd primes q and q'.

The local images for $\mathrm{Sel}^\phi(E/\mathbf{Q})$ are given as follows:

- $\operatorname{im} \delta_\infty = \begin{cases} \mathbf{R}^\times/\mathbf{R}^{\times 2} & \text{if } A < 0, \\ \{1\} & \text{if } A \geq 0; \end{cases}$
- $\operatorname{im} \delta_p = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for odd primes $p \mid \Delta$;
- $\operatorname{im} \delta_p = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \nmid \Delta$;

- $\operatorname{im} \delta_2 = \{1, 5\}$.

Now we assume $d = -2$. As the Hilbert symbol $\left(A^2 - 64, -2\right)_{\mathbf{Q}_2}$ always attains 1 because $A^2 - 64 \equiv 1 \pmod 8$, we have $i_2 = 2$. By Heegner hypothesis, each odd primes dividing $A^2 - 64$ must have $1 = \left(\frac{-2}{p}\right)$, and thus either $p \equiv 1 \pmod 8$ or $p \equiv -5 \pmod 8$. Such p must divide either $A - 8$ or $A + 8$, and these two are congruent to 1 or 5 modulo 8, there must be even number of odd primes (counting multiplicity) congruent to -5 modulo 8 dividing $A \pm 8$. Local images of the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$ are given as follows.

- $\operatorname{im} \delta_\infty^d = \begin{cases} \mathbf{R}^\times/\mathbf{R}^{\times 2} & \text{if } A > 0, \\ \{1\} & \text{if } A \leq 0. \end{cases}$
- $\operatorname{im} \delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \nmid \Delta$.
- $\operatorname{im} \delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \mid \Delta$.
- $\operatorname{im} \delta_2^d = \{1, -2u\}$, for some $u \equiv 1 \pmod 4$.

By the above consideration, we are always able to find a non-trivial element in Φ.

Assume either $d = -q \equiv 3 \pmod 4$ or $d = -2q$ for an odd prime q. Then the prime 2 is ramified in K, and $i_2 = 2$. Notice that we always have $i_q \geq 1$, whence $\sum i_\ell \geq 4$.

Now assume $d = -q \equiv 1 \pmod 4$, so the prime 2 is unramified in K, whence $i_2 = 0$. Let p be an odd prime dividing $A^2 - 64$. Since p must split completely in K, we have $\left(\frac{d}{p}\right) = 1$. Then, $1 = \left(\frac{d}{p}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) = \left(\frac{p}{q}\right)$. Since $\left(\frac{A^2 - 64}{q}\right)$ is the product of such $\left(\frac{p}{q}\right)$, we have $\left(\frac{A^2 - 64}{q}\right) = 1$. This means that $i_q = 2$. The local images for $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$ are given as follows:

- $\operatorname{im} \delta_\infty^d = \begin{cases} \mathbf{R}^\times/\mathbf{R}^{\times 2} & \text{if } A > 0, \\ \{1\} & \text{if } A \leq 0; \end{cases}$
- $\operatorname{im} \delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \nmid \Delta q$;

- $\operatorname{im} \delta_p^d = \mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$ for odd primes $p \mid \Delta$;
- $\operatorname{im} \delta_q^d = \begin{cases} \{1, qu\} & \text{for some } u \in \mathbf{Z}_q^\times, \text{ if } q \nmid A, \\ \mathbf{Q}_q^\times / \mathbf{Q}_q^{\times 2} & \text{if } q \mid A; \end{cases}$
- $\operatorname{im} \delta_2^d = \{1, 5\}$.

So the image of $A - 8$ for example is non-trivial in Φ.

Finally, suppose that $d = -qq'$ for distinct odd primes q and q'. If the prime 2 is ramified in $K = \mathbf{Q}(\sqrt{d})$ then we have $\sum i_\ell \geq 4$. So we can assume $d \equiv 1 \pmod 4$. Without loss of generality, we may assume $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$. For the similar reasons, we also assume $\left(\frac{A^2-64}{q}\right) = \left(\frac{A^2-64}{q'}\right) = -1$. By Heegner hypothesis, if p is an odd prime dividing $A^2 - 64$, then $1 = \left(\frac{-qq'}{p}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} (-1)^{\frac{p-1}{2}\frac{q'-1}{2}} \left(\frac{p}{q}\right)\left(\frac{p}{q'}\right) = \left(\frac{p}{q}\right)\left(\frac{p}{q'}\right)$ and thus we have either $\left(\frac{p}{q}\right) = \left(\frac{p}{q'}\right) = 1$ or $\left(\frac{p}{q}\right) = \left(\frac{p}{q'}\right) = 1$. For the Selmer group $\operatorname{Sel}^{\phi_d}(E_d/\mathbf{Q})$, we have the following:

- $\operatorname{im} \delta_\infty^d = \begin{cases} \mathbf{R}^\times / \mathbf{R}^{\times 2} & \text{if } A > 0, \\ \{1\} & \text{if } A \leq 0; \end{cases}$
- $\operatorname{im} \delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2} / \mathbf{Q}_p^{\times 2}$ for odd primes $p \nmid \Delta qq'$;
- $\operatorname{im} \delta_p^d = \mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$, for odd primes $p \mid \Delta$;
- $\operatorname{im} \delta_q^d = \begin{cases} \{1, qu\} & \text{for some } u \in \mathbf{Z}_q^\times, \text{ if } q \mid A, \\ \mathbf{Q}_q^\times / \mathbf{Q}_q^{\times 2} & \text{if } q \nmid A; \end{cases}$
- $\operatorname{im} \delta_{q'}^d = \begin{cases} \mathbf{Z}_{q'}^\times \mathbf{Q}_{q'}^{\times 2} / \mathbf{Q}_{q'}^{\times 2} & \text{if } q \mid A, \\ \mathbf{Q}_{q'}^\times / \mathbf{Q}_{q'}^{\times 2} & \text{if } q \nmid A; \end{cases}$
- $\operatorname{im} \delta_2^d = \{1, 5\}$.

As $\left(\frac{A-8}{q}\right)\left(\frac{A+8}{q}\right) = -1$, the image of either $A-8$ or $A+8$ contained in Φ is non-trivial. □

Proposition 4.37. *Suppose that $B = -16$. By the considerations of the subsection above, we assume*

- $A \equiv 1 \pmod 4$, *and*
- *if ℓ is an odd prime dividing $A^2 - 4B = A^2 + 64$, then it has odd exponent.*

Then we have $\sum i_\ell + \dim_{\mathbf{F}_2} \Phi \geq 4$, i.e., $2 \mid (\#Ш(E/K))^{1/2}$, except for

- $A = 15$, *in this case the curve is '272b2' having $C_2 = 2$;*
- *the family characterised by the condition that $A^2 + 64$ is a prime, having $M = 2$ for any curve in this family.*

Proof. Our elliptic curve E is given by

$$y^2 = x^3 + Ax^2 - 16x, \tag{4.20}$$

such that $A \equiv 1 \pmod 4$. The above equation has discriminant $\Delta = 2^{12}\left(A^2+64\right)$, whereas the minimal discriminant of the curve is given by $\Delta_{\min} = 2^{-12}2^4(2^4)^2(A^2 + 4\cdot 2^4) = A^2 + 2^6$. We have assumed moreover that $\Delta_{\min} > 0$. Note that the prime 2 is always a good prime for E. Note that by the sum of two squares theorem, there are no odd prime divisors of $A^2 + 64$ congruent to 3 modulo 4.

By Lemma 5.5 of Cao–Chu–Shiu [CCS], if we have $A^2+64 = p^k$ for some $k \in \mathbf{Z}_{\geq 1}$, then $k = 1$ unless $A = 15$, $p = 17$, and $e = 2$. This corresponds to the curve '272b2', having $C_2 = 4$. This allows us to assume that either A^2+64 is a prime or it has at least two distinct prime divisors. Suppose first that $A^2 + 64$ is a prime. Then the curves are called Neumann–Setzer curves, and in [StWa04], Stein and Watkins proved that the Manin constant $M = 2$. From now on, we assume there are at least two distinct odd prime divisors of $A^2 + 64$.

Now we consider local norm indices. Clearly, $i_\infty = 1$. When the prime 2 is ramified in K, then $i_2 = 2$, since $A^2+64 \equiv 1 \pmod 8$. So we do not need to consider those cases when 2 is ramified, unless $d = -2$. We only consider the following cases for d:

- $d = -2$;
- $d = -q \equiv 1 \pmod 4$, for an odd prime q;
- $d = -qq' \equiv 1 \pmod 4$, for odd primes q and q'.

The local images for $\mathrm{Sel}^{\phi}(E/\mathbf{Q})$ are given as follows:

- $\operatorname{im} \delta_\infty = \{1\}$;
- $\operatorname{im} \delta_p = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for odd primes $p \mid \Delta$;
- $\operatorname{im} \delta_p = \mathbf{Z}_p^\times\mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \nmid \Delta$;
- $\operatorname{im} \delta_2 = \{1, 5\}$.

Now assume $d = -2$. As already noted, $i_2 = 2$ in this case. By Heegner hypothesis, each odd primes p dividing $A^2 + 64$ must have $1 = \left(\frac{-2}{p}\right)$, and thus $p \equiv 1 \pmod 8$. Local images of the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$ are given as follows.

- $\operatorname{im} \delta_\infty^d = \{1\}$.
- $\operatorname{im} \delta_p^d = \mathbf{Z}_p^\times\mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \nmid \Delta$.
- $\operatorname{im} \delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$, for any odd primes $p \mid \Delta$.
- $\operatorname{im} \delta_2^d = \{1\}$.

Thus the image of any prime dividing Δ in Φ is non-trivial.

Let $d = -q \equiv 1 \pmod 4$. The prime 2 is unramified in K, whence $i_2 = 0$. Let p be an odd prime dividing $A^2 + 64$. Since p must split completely in K, we have $\left(\frac{d}{p}\right) = 1$. Then, $1 = \left(\frac{d}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) = \left(\frac{p}{q}\right)$. Since $\left(\frac{A^2+64}{q}\right)$ is the product of such $\left(\frac{p}{q}\right)$, we have $\left(\frac{A^2+64}{q}\right) = 1$. This means that $i_q = 2$. The local images for $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$ are given as follows:

- $\operatorname{im} \delta_\infty^d = \{1\}$;

- $\operatorname{im} \delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \nmid \Delta q$.
- $\operatorname{im} \delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for odd primes $p \mid \Delta$;
- $\operatorname{im} \delta_q^d = \{1\}$;
- $\operatorname{im} \delta_2^d = \{1, 5\}$.

Since $\left(\dfrac{p}{q}\right) = 1$ for any odd prime $p \mid \Delta$, its image in Φ must be non-trivial.

Finally, assume $d = -qq' \equiv 1 \pmod 4$, for odd primes q and q'. If the prime 2 is ramified in $K = \mathbf{Q}(\sqrt{d})$ then we have $\sum i_\ell \geq 4$. So we can assume $d \equiv 1 \pmod 4$, which means, the modulo 4 residues of q and q' must be different. Thus we assume $q \equiv 1 \pmod 4$ and $q' \equiv 3 \pmod 4$. Moreover, for similar reasons, we assume $\left(\frac{A^2+64}{q}\right) = \left(\frac{A^2+64}{q'}\right) = -1$. If, moreover, $q \mid A$, then we have $-1 = \left(\dfrac{A^2+64}{q}\right) = \left(\dfrac{64}{q}\right) = 1$, a contradiction. So we can also assume $q \nmid A$. For the Selmer group $\mathrm{Sel}^{\phi_d}(E_d/\mathbf{Q})$, we have the following:

- $\operatorname{im} \delta_\infty^d = \{1\}$;
- $\operatorname{im} \delta_p^d = \mathbf{Z}_p^\times \mathbf{Q}_p^{\times 2}/\mathbf{Q}_p^{\times 2}$ for odd primes $p \mid \Delta q$ (including $p = q'$);
- $\operatorname{im} \delta_p^d = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for odd primes $p \mid \Delta q$;
- $\operatorname{im} \delta_2^d = \{1, 5\}$.

Again, the image of a prime dividing Δ in Φ is non-trivial. This concludes the proof. □

4.7.3 Exceptional case

In this case we deal with the cases where $A^2 + 4$ is a power of an odd prime. By Lemma 5.4 of Cao–Chu–Shiu [CCS], then $A^2 + 4$ is a prime unless either $A = 2$ or $A = 11$. For those two non-prime cases, the corresponding curves are '128d2' and '80b4', and both of them have Manin constant 2. Excluding these cases, we assume $A^2 + 4$ is a prime.

This family is parametrised by the following Weierstrass equation: $y^2 = x^3 + Ax^2 - x$, where A is an integer not divisible by 4, and $A^2 + 4 = p$ is an odd prime. It has discriminant $\Delta = 16(A^2 + 4) = 16p$, which is the minimal discriminant. The conductor of the curve E is $4p$ and $E(\mathbf{Q})_{\text{tors}} = \mathbf{Z}/2\mathbf{Z}$.

Let $G = E(\mathbf{Q})_{\text{tors}} \cong \mathbf{Z}/2\mathbf{Z}$, and consider the curve $E' := E/G$. By Vélu's formula, we can find a Weierstrass equation for E'. This is given as follows:

$$y^2 = x^3 + Ax^2 + 4x + 4A$$

with discriminant $\Delta' = -2^8(A^2 + 4)^2 = -2^8p^2$. As the 2-torsion polynomial for E' is given by

$$4(x^2 + 4)(x + A),$$

we must have a rational 2-torsion point $P = (-A, 0) \in E'(\mathbf{Q})$, i.e., $\mathbf{Z}/2\mathbf{Z} \subseteq E'(\mathbf{Q})_{\text{tors}}$. If $E'(\mathbf{Q})_{\text{tors}} \supsetneq \mathbf{Z}/2\mathbf{Z}$, the weak Gross–Zagier conjecture is proved in the above sections. So we assume $E'(\mathbf{Q}) = \mathbf{Z}/2\mathbf{Z}$. Making a change of variables $x \mapsto x' = x + A$, we get another Weierstrass equation

$$y^2 = x^3 - 2Ax^2 + (A^2 + 4)x.$$

By Tate's algorithm, we know that $C_p = 2$. Thus the weak Gross–Zagier conjecture is true for E' unconditionally.

Now we consider $E'(K)_{\text{tors}}$ for quadratic field K satisfying Heegner hypothesis. If $\operatorname{ord}_2 E'(K)_{\text{tors}} > \operatorname{ord}_2 E'(\mathbf{Q})_{\text{tors}}$, then $E'(K)$ must contain either $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ or $\mathbf{Z}/4\mathbf{Z}$. For the first case, the 2-torsion polynomial of E' must split into linear factors in K. As the polynomial is $4(x^2+4)(x+A)$, this happens if and only if $K = \mathbf{Q}(\sqrt{-1})$. But in this case $u_K = 2$, and the weak conjecture is also true for E.

Now suppose that $E(K)_{\text{tors}} \geq \mathbf{Z}/4\mathbf{Z}$. By Lemma 13 in [GJTo], we must have $A^2 + 4 = s^2$ for some $s \in \mathbf{Q}$. But since $A^2 + 4 = p$ is a prime, we cannot have this case. Therefore, we have the following corollary to Proposition 4.16.

Corollary 4.38. *The weak Gross–Zagier conjecture is true for E in this family and for any quadratic field K satisfying Heegner hypothesis.*

Bibliography

[Abh] S. S. Abhyankar, *Resolution of singularities of arithmetical surfaces*, in: O. F. G. Schilling ed., *Arithmetical algebraic geometry*, Proceedings of a Conference Held at Purdue University (1963), Harper & Row, 1965.

[ARS] A. Agashe, K. Ribet, W. Stein, *The Manin constant*, Pure and Applied Mathematics Quarterly, **2** (2006), pp. 617 – 636.

[Art] M. Artin, *Néron models*, in: G. Cornell, J. H. Silverman eds., *Arithmetic geometry*, Springer, 1986.

[AtLe] A. O. L. Atkin, J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Mathematische Annalen, **185** (1970), pp. 135 – 160.

[Bir] B. J. Birch, *Cyclotomic fields and Kummer extensions*, in: J. W. S. Cassels, A. Fröhlich eds., *Algebraic number theory*, Proceedings of an instructional conference organised by the London Mathematical Society, Thompson Book Company Inc., 1967.

[BLR] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete 3. Folge, Band 21, Springer, 1990.

[BCDT] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* **Q***: wild 3-adic exercises*, Journal of the American Mathematical Society, **14** (2001), pp. 843 – 939.

[ByKi] D. Byeon, T. Kim, *Optimal curves differing by a 5-isogeny*, Acta Arithmetica, **165** (2014), pp. 351 – 359.

[BKY] D. Byeon, T. Kim, D. Yhee, *On a conjecture of Gross and Zagier*, preprint, available at `http://arxiv.org/abs/1501.06296`.

[ByYh11] D. Byeon, D. Yhee, *Rational torsion on optimal curves and rank-one quadratic twists*, Journal of Number Theory, **131** (2011), pp. 552 – 560.

[ByYh13] ————————, *Optimal curves differing by a 3-isogeny*, Acta Arithmetica, **158** (2013), pp. 219 – 227.

[CCS] Z. Cao, C. I. Chu, W. C. Shiu, *The exponential diophantine equation* $AX^2 + BY^2 = \lambda k^Z$ *and its applications*, Taiwanese Journal of Mathematics, **12** (2008), pp. 1015 – 1034.

[Car] H. Carayol, *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet*, in: B. Mazur, G. Stevens eds., *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture*, Contemporary Mathematics **165**, American Mathematical Society, 1994.

[Cas62] J. W. S. Cassels, *Arithmetic on curves of genus 1, IV, Proof of the Hauptvermutung*, Journal für die reine und angewandte Mathematik, **211** (1962), pp. 95–112.

[Cas65] ————————, *Arithmetic on curves of genus 1, VIII, On the conjectures of Birch and Swinnerton-Dyer*, Journal für die reine und angewandte Mathematik, **217** (1965), pp. 180 – 189.

[Cre] J. E. Cremona, *Elliptic curve data*, updated 2015-10-31, available at `http://johncremona.github.io/ecdata/`.

[Dar97] H. Darmon, *Wiles' theorem and the arithmetic of elliptic curves*, in: G. Cornell, J. H. Silverman, G. Stenvens eds., *Modular forms and Fermat's last theorem*, Springer, 1997.

[Dar04] ————————, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics **101**, American Mathematical Society, 2004.

[DDT] H. Darmon, F. Diamond, R. Taylor, *Fermat's last theorem*, in. R. Bott et al. eds., *Current Development in Mathematics, 1995*, International Press, 1994.

[DiIm] F. Diamond, J. Im, *Modular forms and modular curves*, in: V. K. Murty ed., *Seminar on Fermat's last theorem*, Canandian Mathematical Society Conference Proceedings **17**, American Mathematical Society, 1995.

[Dok] T. Dokchitser, *Notes on parity conjecture*, in: L. Berger et al., *Elliptic curves, Hilbert modular forms and Galois deformations*, Advanced courses in Mathematics – CRM Barcelona, Springer, 2003.

[DoDo] T. Dokchitser, V. Dokchitser, *Local invariants of isogenous elliptic curves*, Transactions of the American Mathematical Society, **367** (2015), pp. 4339 – 4358.

[Dum] N. Dummigan, *Rational torsion on optimal curves*, International Journal of Number Theory, **1** (2005), pp. 513 – 531.

[Fal] G. Faltings, *Finiteness theorems for abelian varieties over number fields*, in: G. Cornell, J. H. Silverman eds., *Arithmetic geometry*, Springer, 1986.

[Fu] L. Fu, *Étale cohomology theory*, Nankai tracts in Mathematics **13**, World Scientific Publishing Co., 2011.

[GJTo] E. González-Jiménez, J. M. Tornero, *Torsion of rational elliptic curves over quadratic fields II*, Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales, Serie A. Matemática, to appear.

[Got] T. Goto, *A study on the Selmer groups of elliptic curves with a rational 2-torsion*, Doctoral thesis, Kyushu University, 2002.

[Gro84] B. H. Gross, *Heegner points on $X_0(N)$*, in: R. A. Rankin ed., *Modular forms*, Ellis Horwood Ltd., 1984.

[Gro91] ————————, *Kolyvagin's work on modular elliptic curves*, in: J. Coates, M. J. Taylor eds., *L-functions and arithmetic*, London Mathematical Society Lecture Notes Series **153**, Cambridge University Press, 1991.

[Gro11] ————————, *Lectures on the conjecture of Birch and Swinnerton-Dyer*, in: C. Popescu, K. Rubin, A. Silverberg eds., *Arithmetic of L-functions*, IAS/Park City Mathematics Series **18**, American Mathematical Society, 2011.

[GrZa] B. H. Gross, D. B. Zagier, *Heegner points and derivatives of L-series*, Inventiones Mathematicae, **84** (1986), pp. 225 – 320.

[Had] T. Hadano, *Elliptic curves with torsion point*, Nagoya Mathematical Journal, **66** (1977), pp. 99 – 108.

[Har] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer, 2010.

[HiSi] M. Hindry, J. H. Silverman, *Diophantine geometry: an introduction*, Graduate Texts in Mathematics **201**, Springer, 2000.

[Kam] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Inventiones Mathematicae, **109** (1992), pp. 221 – 229.

[Ken] M. A. Kenku, *On the number of* $\mathbf{Q}$*-isomorphism classes of elliptic curves in each* $\mathbf{Q}$*-isogeny class*, Journal of Number Theory, **15** (1982), pp. 199 – 202.

[KeMo] M. A. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Mathematical Journal, **109** (1988), pp. 125 – 149.

[KlSc] R. Kloosterman, E. F. Schaefer, *Selmer groups of elliptic curves that can be arbitrarily large*, Journal of Number Theory, **99** (2003), pp. 148 – 163.

[Kna] A. W. Knapp, *Elliptic curves*, Mathematical Notes **40**, Princeton University Press, 1992.

[Kod64] K. Kodaira, *On the structure of compact complex analytic surfaces I*, American Journal of Mathematics, **86** (1964), pp. 751 – 798.

[Kod66] ————————, *On the structure of compact complex analytic surfaces II*, American Journal of Mathematics, **88** (1966), pp. 682 – 721.

[Kol] V. A. Kolyvagin, *On the Mordell–Weil group and the Shafarevich–Tate group of modular elliptic curves*, Proceedings of the International Congress of Mathematicians (Kyoto, 1990).

[Kra] K. Kramer, *Arithmetic of elliptic curves upon quadratic extension*, Transactions of the American Mathematical Society, **264** (1981), pp. 121 – 135.

[Kub] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proceedings of the London Mathematical Society, **s3-33** (1976), pp. 193 – 237.

[LiOe] S. Ling, J. Oesterlé, *The Shimura subgroup of $J_0(N)$*, Astérisque, **6** (1991), pp. 171 – 203.

[Lip] J. Lipman, *Desingularization of two-dimensional schemes*, Annals of Mathematics, **90** (1968), pp. 151 – 207.

[Liu] Q. Liu, *Algebraic geometry and arithmetic curves*, translated form French by R. Erné, Oxford Graduate Texts in Mathematics **6**, Oxford University Press Inc., 2006.

[Lor] D. Lorenzini, *Torsion and Tamagawa numbers*, Annales de l'institut Fourier, **61** (2011), pp. 1995 – 2037.

[Man] J. I. Manin, *Parabolic points and zeta functions of modular curves*, Izvestiya Akademii Nauk SSSR Seriya Matematicheskaya, **36** (1972), pp. 19 – 66.

[Maz72a] B. Mazur, *Courbes elliptiques et symboles modulaires*, Séminaire N. Bourbaki, 1971/72 no. 414, pp. 277 – 294.

[Maz72b] ————————, *Rational points of abelian varieties with values in towers of number fields*, Inventiones Mathematicae, **18** (1972), pp. 183 – 266.

[Maz77] ————————, *Modular curves and the Eisenstein ideal*, Publications Mathématiques de l'Institut Hautes Études Scientifiques, **47** (1977), pp. 33 – 186.

[Maz78] ————————, *Rational isogenies of prime degree*, Inventiones Mathematicae, **44** (1978), pp. 129 – 162.

[MaRa] B. Mazur, M. Rapport, *Behavior of the Néron model of the jacobian of $X_0(N)$ at bad primes*, appendix to [Maz77].

[MaSe] B. Mazur, J.-P. Serre, *Points rationnels des courbes modulaires $X_0(N)$*, Séminaire N. Bourbaki, 1974/75 no. 469, pp. 238 – 255.

[MeOe] J.-F. Mestre, J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance m-ième*, Journal für die reine und angewandte Mathematik, **400** (1989), pp. 173 – 184.

[Mil80] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series **33**, Princeton University Press, 1980.

[Mil06] ————————, *Elliptic curves*, BookSurge Publishers, 2006.

[MMR] J. M. Miret, R. Moreno, A. Rio, *Generalization of Vélu's formulae for isogenies between elliptic curves*, in: J. González et al. eds., *Proceedings of the "Primeras Jornadas de Teoría de Números"* (Barcelona, 2005), Publicacions Matemàtiques, Universitat Autònoma de Barcelona, 2007.

[Mum] D. Mumford, *The red book of varieties and schemes*, Second, expanded edition, Lecture Notes in Mathematics **1358**, Springer, 1999.

[Naj] F. Najman, *The number of twists with large torsion of an elliptic curve*, Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales, Serie A. Matemáticas, to appear.

[Nér] A. Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Publications Mathématiques de l'Institut Hautes Études Scientifiques, **21** (1964), pp. 5 – 128.

[Neu99] J. Neukirch, *Algebraic number theory*, translated from German by N. Schappacher, Grundlehren der mathematischen Wissenschaften **322**, Springer, 1999.

[Neu03] ————————, *Class field theory: The Bonn lectures*, edited by A. Schmidt, translated from German by F. Lemmermeyer and W. Snyder, Springer, 2013.

[Neum] O. Neumann, *Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten II*, Mathematische Nachrichten, **56** (1973), pp. 269 – 280.

[Roh] D. E. Rohrlich, *Modular curves, Hecke correspondences, and L-functions*, in: G. Cornell, J. H. Silverman, G. Stenvens eds., *Modular forms and Fermat's last theorem*, Springer, 1997.

[RuSi] K. Rubin, A. Silverberg, *Families of elliptic curves with constant mod p representaion*, in: J. H. Coates, S.-T. Yau eds., *Elliptic curves, modular forms, and Fermat's last theorem*, International Press, 1997.

[Sai03] T. Saito, *Fermat's last theorem: Basic tools*, Translations of Mathematical Monographs **243**, American Mathematical Society, 2013.

[Sai04] ————————, *Fermat's last theorem: The proof*, Translations of Mathematical Monographs **245**, American Mathematical Society, 2014.

[Ser67] J.-P. Serre, *Complex multiplication*, in: J. W. S. Cassels, A. Fröhlich eds., *Algebraic number theory*, Proceedings of an instructional conference organised by the London Mathematical Society, Thompson Book Company Inc., 1967.

[Ser72] ————————, *Propriétés galoisienne des points d'ordre fini des courbes elliptiques*, Inventiones Mathematicae, **15** (1972), pp. 259 – 331.

[Ser79] ————————, *Local fields*, translated from French by M. J. Greenberg, Graduate Texts in Mathematics **67**, Springer, 1979.

[Set] B. Setzer, *Elliptic curves of prime conductor*, Journal of the London Mathematical Society, **s2-10** (1975), pp. 367 – 378.

[Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, 1994.

[Sil97] ————————, *A survey of the arithmetic theory of elliptic curves*, in: G. Cornell, J. H. Silverman, G. Stenvens eds., *Modular forms and Fermat's last theorem*, Springer, 1997.

[Sil09] ————————, *The arithmetic of elliptic curves*, second edition, Graduate Texts in Mathematics **106**, Springer, 2009.

[SAGE] W. Stein et al., *Sage Mathematics Software*, The Sage Development Team, 2015, `http://www.sagemath.org`.

[StWa02] W. A. Stein, M. Watkins, *A database of elliptic curves—first report*, in: C. Fieker, D. R. Kohel eds., *Algorithmic Number Theory*, Proceedings of the 5th International Symposium, ANTS-V (Sydney, 2002), Lecture Notes in Computer Science **2369**, Springer, 2002.

[StWa04] ————————, *Modular parametrizations of Neumann–Setzer elliptic curves*, International Mathematics Research Notices, **2004**, pp. 1395 – 1405.

[Ste] G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, Inventiones Mathematicae, **98** (1989), pp. 75 – 106.

[Tat74] J. Tate, *Arithmetic of elliptic curves*, Inventiones Mathematicae, **23** (1974), pp. 179 – 206.

[Tat75] ————————, *Algorithm for determining the types of a singular fiber in an elliptic pencil*, in: B. J. Birch, W. Kuyk eds., *Modular functions of one variable IV*, Proceedings of the International Summer School (University of Antwerp, RUCA, 1972), Lecture Notes in Mathematics **476**, Springer, 1975.

[TaWi] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Mathematics, **141** (1995), pp. 553 – 572.

[Vat] V. Vatsal, *Multiplicative subgroup of $J_0(N)$ and applications to elliptic curves*, Journal de l'Institut de Mathématiques de Jussieu, **4** (2005), pp. 281 – 316.

[Wil] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Mathematics, **141** (1995), pp. 443 – 551.

국문초록

이 논문의 목표는 다음 두 가지 타원 곡선의 수론에 관련된 추측을 증명하는 것이다. 하나는 5-동종함수(同種函數, isogeny)에 대한 스타인–왓킨스 추측이고, 다른 하나는 그로스–자기에 추측이다.

본질적으로 스타인–왓킨스 추측은 주어진 타원 곡선의 유리 동종함수류(同種函數類, isogeny class)에 소속된 두 가지 종류의 최적타원곡선(optimal elliptic curve)들 사이의 관계를 다루는 것이다. 이 논문에서는 이러한 두 가지 최적타원곡선이 실제로 동형이 아니게 되어 5-동종함수로 달라지게 되는 경우는 동종함수류가 '11a'라 불리는 특별한 경우일 때 뿐이라는 것을 보인다.

그로스–자기에 추측은 유명한 버츠–스위너튼-다이어 추측으로부터 유래하였다. 버츠–스위너튼-다이어 추측에 그로스와 자기에의 결과를 합성하여 만들어진 이 추측은 증명될 경우 버츠–스위너튼-다이어의 강한 형태에 대한 이론적인 증거를 주게 된다. 타원곡선이 특정한 형태의 유리 꼬임 부분군(rational torsion subgroup)을 가질 때, 이 논문에서는 이 그로스–자기에 추측의 증명을 다룬다. 즉, 꼬임 부분군의 위수가 본래 타원곡선이 지니고 있는 적당한 수론적 불변량을 나눈다는 것을 보인다.

주요어휘: 타원 곡선, 버츠와 스위너튼-다이어 추측, 그로스–자기에 정리, 타원 곡선의 동종함수
학번: 2009–20265